Footprinting i rozpoznanie

Footprinting odnosi się do zebrania jak największej ilości informacji o sieci docelowej z publicznie dostępnych źródeł.

Scenariusz laboratoryjny

Rekonesans odnosi się do zbierania informacji o celu, co jest pierwszym krokiem każdego ataku na system. Ma swoje korzenie w operacjach wojskowych, gdzie termin ten odnosi się do misji zbierania informacji o wrogu. Rekonesans pomaga atakującym zawęzić zakres ich wysiłków i pomaga w doborze broni ataku. Atakujący wykorzystują zebrane informacje do stworzenia planu lub „śladu" organizacji, który pomaga im wybrać najskuteczniejszą strategię naruszenia bezpieczeństwa systemu i sieci. Podobnie ocena bezpieczeństwa systemu lub sieci rozpoczyna się od rekonesansu i rozpoznania celu. Etyczni hakerzy i testerzy penetracyjni muszą zebrać wystarczającą ilość informacji o celu oceny przed rozpoczęciem oceny. Etyczni hakerzy i testerzy penetracyjni powinni symulować wszystkie kroki, które zwykle wykonuje atakujący, aby uzyskać rzetelne wyobrażenie o stanie bezpieczeństwa atakowanej organizacji. W tym scenariuszu pracujesz jako etyczny haker w dużej organizacji. Twoja organizacja jest zaniepokojona doniesieniami o nowych wektorach ataków nękających duże organizacje na całym świecie. Ponadto Twoja organizacja była w przeszłości celem poważnego naruszenia bezpieczeństwa, w wyniku którego dane osobowe kilku jej klientów zostały ujawnione w serwisach społecznościowych. Menedżerowie wyższego szczebla poprosili Cię o przeprowadzenie proaktywnej oceny bezpieczeństwa firmy. Zanim rozpoczniesz jakąkolwiek ocenę, powinieneś omówić i zdefiniować zakres z kierownictwem; zakres oceny identyfikuje systemy, sieć, zasady i procedury, zasoby ludzkie oraz wszelkie inne komponenty systemu, które wymagają oceny bezpieczeństwa. Powinieneś także uzgodnić z kierownictwem zasady zaangażowania (RoE) – „co robić, a czego nie" w ocenie. Po uzyskaniu niezbędnych zgód do przeprowadzenia etycznego hakowania należy rozpocząć zbieranie informacji o docelowej organizacji. Po metodologicznym rozpoczęciu procesu śledzenia uzyskasz plan profilu bezpieczeństwa docelowej organizacji. Termin „plan" odnosi się do unikalnego profilu systemu docelowej organizacji będącego wynikiem śladu. Laboratoria w tym module zapewnią Ci doświadczenie w czasie rzeczywistym w zbieraniu różnych informacji o docelowej organizacji z różnych otwartych lub publicznie dostępnych źródeł.

Cel laboratorium

Celem laboratorium jest wyodrębnienie informacji o organizacji docelowej, które obejmują między innymi:

• Informacje o organizacji: Dane pracowników, adresy i dane kontaktowe, dane partnerów, łącza internetowe, technologie internetowe, patenty, znaki towarowe itp.

• Informacje o sieci: domeny, subdomeny, bloki sieciowe, topologie sieci, zaufane routery, zapory ogniowe, adresy IP osiągalnych systemów, rekord Whois, rekordy DNS i inne powiązane informacje

• Informacje o systemie: systemy operacyjne, systemy operacyjne serwerów sieciowych, lokalizacja serwerów sieciowych, konta użytkowników i hasła itp.

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Maszyna wirtualna Parrot Security

* Maszyna wirtualna Windows Server 2019

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 220 minut

Przegląd Footprintingu

Footprinting odnosi się do procesu zbierania informacji o sieci docelowej i jej środowisku, co pomaga w ocenie stanu bezpieczeństwa infrastruktury IT docelowej organizacji. Pomaga również określić poziom ryzyka związanego z publicznie dostępnymi informacjami organizacji. Footprinting można podzielić na pasywny i aktywny:

Pasywny Footprintig : obejmuje zbieranie informacji bez bezpośredniej interakcji. Ten typ odcisku stopy jest zasadniczo przydatny, gdy istnieje wymóg, aby działania związane ze zbieraniem informacji nie zostały wykryte przez cel.

Aktywny Footprinting: obejmuje zbieranie informacji z bezpośrednią interakcją. W przypadku aktywnego śladu cel może rozpoznać trwający proces gromadzenia informacji, ponieważ jawnie wchodzimy w interakcje z siecią docelową.

Zadania laboratoryjne

Etyczni hakerzy lub testerzy penetracyjni używają wielu narzędzi i technik do zbierania informacji o celu. Zalecane zadania , które pomogą Ci w nauce różnych technik footprintingu, obejmują:

1 Wykonaj śledzenie śladu za pośrednictwem wyszukiwarek

1.1 Zbierz informacje za pomocą zaawansowanych technik Google Flacking

1.2 Zbierz informacje z wyszukiwarek wideo

1.3 Zbierz informacje z wyszukiwarek FTP

1.4 Zbieranie informacji z wyszukiwarek loT

2 Wykonaj Footprinting poprzez usługi sieciowe

2.1 Znajdź domeny i subdomeny firmy za pomocą Netcraft

2.2 Zbieranie danych osobowych za pomocą usługi PeekYou Online People Search

2.3 Zbierz listę e-mailową za pomocą Flarvester

2.4 Zbieranie informacji za pomocą wyszukiwania w głębokiej i ciemnej sieci

2.5 Określanie docelowego systemu operacyjnego poprzez bierny ślad

3 Wykonaj Footprinting za pośrednictwem portali społecznościowych

3.1 Zbieraj informacje o pracownikach z Linkedln za pomocą Harvester

3.2 Zbieraj dane osobowe z różnych serwisów społecznościowych za pomocą programu Sherlock

3.3 Zbierz informacje za pomocą Followerwonk

4 Wykonaj Footprinting strony internetowej

4.1 Zbierz informacje o witrynie docelowej za pomocą narzędzia Ping Command Line Utility

4.2 Zbierz informacje o Stronie docelowej za pomocą Photon

4.3 Zbierz informacje o Witrynie docelowej za pomocą Central Ops

4.4 Wyodrębnij dane firmy za pomocą narzędzia Web Data Extractor

4.5 Kopiuj witrynę docelową za pomocą narzędzia FITTrack Web Site Copier

4.6 Zbierz informacje o witrynie docelowej za pomocą GRecon

4.7 Zbierz listę słów ze strony docelowej za pomocą CeWL

5 Wykonaj śledzenie adresu e-mail

5.1 Zbierz informacje o celu, śledząc wiadomości e-mail za pomocą eMailTrackerPro

6 Wykonaj Whois Footprinting

6.1 Wykonaj wyszukiwanie Whois za pomocą DomainTools

7 Wykonaj funkcję DNS Footprinting

7.1 Zbierz informacje DNS za pomocą narzędzia wiersza poleceń nslookup i narzędzia online w wersji

7.2 Wykonaj odwrotne wyszukiwanie DNS przy użyciu funkcji Reverse IP Domain Check i DNSRecon

7.3 Zbierz informacje o subdomenach i rekordach DNS za pomocą SecurityTrails

8 Wykonaj analizę śladu sieciowego

8.1 Zlokalizuj zasięg sieci

8.2 Wykonywanie trasowania sieciowego na komputerach z systemem Windows i Linux

8.3 Wykonaj zaawansowane śledzenie tras sieciowych za pomocą Path Analyzer Pro

9 Wykonaj Footprinting za pomocą różnych narzędzi Footprinting

9.1 Śledzenie śladu celu za pomocą Recon-ng

9.2 Wyznaczanie śladu celu za pomocą Maltego

9.3 Określanie śladu celu za pomocą OSRFramework

9.4 Wyznaczanie śladu celu za pomocą FOCA

9.5 Wyznaczanie śladu celu za pomocą BillCipher

9.6 Określanie śladu celu przy użyciu OSINT Framework

Wykonaj Footprinting za pośrednictwem wyszukiwarek

Wyszukiwarki są głównymi źródłami informacji służącymi do wydobywania z Internetu krytycznych informacji o docelowej organizacji.

Scenariusz laboratoryjny

Jako profesjonalny etyczny haker lub tester penetracyjny Twoim pierwszym krokiem jest zebranie jak największej ilości informacji o docelowej organizacji poprzez wykonanie footprintingu za pomocą wyszukiwarek; możesz przeprowadzić zaawansowane wyszukiwanie obrazów, odwrócone wyszukiwanie obrazów, zaawansowane wyszukiwanie wideo itp. Dzięki efektywnemu wykorzystaniu wyszukiwarek możesz wydobyć krytyczne informacje o docelowej organizacji, takie jak platformy technologiczne, dane pracowników, strony logowania, portale intranetowe, dane kontaktowe itp., które pomogą Ci w przeprowadzaniu socjotechniki i innych rodzajów zaawansowanych ataków systemowych.

Cele laboratorium

• Zbieraj informacje, korzystając z zaawansowanych technik hakerskich Google

• Zbieraj informacje z wyszukiwarek wideo

• Zbieraj informacje z wyszukiwarek FTP

• Zbieraj informacje z wyszukiwarek loT

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

• Maszyna wirtualna Windows 11

• Przeglądarki internetowe z połączeniem internetowym

• Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 20 minut

Przegląd wyszukiwarek

Wyszukiwarki używają robotów indeksujących, zautomatyzowanego oprogramowania, które stale skanuje aktywne strony internetowe i dodaje uzyskane wyniki do indeksu wyszukiwarki, który jest dalej przechowywany w ogromnej bazie danych. Gdy użytkownik wysyła zapytanie do indeksu wyszukiwarki, zwraca listę stron wyników wyszukiwania (SERP). Wyniki te obejmują strony internetowe, filmy, obrazy i wiele różnych typów plików uszeregowanych i wyświetlanych na podstawie ich trafności. Przykłady głównych wyszukiwarek to Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha i DuckDuckGo.

Zadania laboratoryjne

Zadanie 1: Zbierz informacje, korzystając z zaawansowanych technik hakerskich Google

Zaawansowane hakowanie w Google odnosi się do sztuki tworzenia złożonych zapytań w wyszukiwarkach poprzez zatrudnianie zaawansowanych operatorów Google do wydobywania poufnych lub ukrytych informacji o firmie docelowej z wyników wyszukiwania Google. Może to dostarczyć informacji o stronach internetowych, które są podatne na wykorzystanie.

Uwaga: W tym przypadku za organizację docelową uznamy EC-Council . Możesz jednak wybrać wybraną przez siebie organizację docelową.

1. Włącz maszynę wirtualną Windows 11.

2. Domyślnie wybrany jest profil użytkownika Admin, wpisz Pa$$wOrd w polu Hasło i naciśnij Enter, aby się zalogować.

Uwaga: Jeśli pojawi się kreator Witamy w systemie Windows, kliknij przycisk Kontynuuj, a w kreatorze logowania za pomocą narzędzia Microsoft kliknij przycisk Anuluj.

Uwaga: Pojawi się ekran Sieci. Kliknij Tak, aby komputer mógł być wykrywany przez inne komputery i urządzenia w sieci.

3. Uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.google.com i naciśnij Enter.

Notatka:

• Jeśli pojawi się wyskakujące okno przeglądarki domyślnej, usuń zaznaczenie pola wyboru Zawsze wykonuj to sprawdzanie podczas uruchamiania przeglądarki Firefox i kliknij przycisk Nie teraz. Jeśli pojawi się powiadomienie, kliknij OK, rozumiem, aby zakończyć przeglądanie informacji.

4. Po wyświetleniu wyszukiwarki Google powinieneś zobaczyć pasek wyszukiwania.

Uwaga: jeśli w prawym górnym rogu pojawi się wyskakujące okienko, kliknij Nie, dziękuję.

5. Wpisz intitledogin site:eccouncil.org i naciśnij Enter. To polecenie wyszukiwania wykorzystuje zaawansowane operatory Google intitle i site, które ograniczają wyniki do stron w witrynie eccouncil.org, które zawierają strony logowania.

Uwaga: w tym przypadku ten operator zaawansowanej wyszukiwarki Google może pomóc atakującym i pe testerom wyodrębnić strony logowania z witryny docelowej organizacji. Atakujący mogą narażać strony logowania na różne ataki, takie jak brutalne wymuszanie danych uwierzytelniających, ataki polegające na wstrzykiwaniu i inne ataki na aplikacje internetowe. Podobnie ocena stron logowania pod kątem różnych ataków ma kluczowe znaczenie dla testów penetracyjnych.

6. Teraz kliknij ikonę Wstecz znajdującą się w lewym górnym rogu okna przeglądarki, aby wrócić do https://www.google.com.

7. W pasku wyszukiwania wpisz polecenie EC-Council filetype:pdf i naciśnij Enter, aby wyszukać wyniki na podstawie rozszerzenia pliku.

Uwaga: Tutaj wyszukiwany jest typ pliku pdf dla organizacji docelowej EC-Council. Wynik może się różnić podczas wykonywania tego zadania.

Uwaga: plik PDF i inne dokumenty z docelowej witryny internetowej mogą zawierać poufne informacje o produktach i usługach docelowych. Mogą pomóc atakującym w określeniu wektora ataku w celu wykorzystania celu.

8. Teraz kliknij dowolny link z wyników (tutaj, pierwszy link), aby wyświetlić plik pdf.

9. Zostanie wyświetlona strona wyświetlająca plik pdf.

10. Oprócz wyżej wymienionych zaawansowanych operatorów Google, możesz również skorzystać z poniższych, aby przeprowadzić wyszukiwanie zaawansowane, aby zebrać więcej informacji o docelowej organizacji z publicznie dostępnych źródeł.

• cache: Ten operator umożliwia przeglądanie wersji strony internetowej zapisanej w pamięci podręcznej. [cache:www.eccouncil.org] – Zapytanie zwraca zapisaną w pamięci podręcznej wersję witryny www.eccouncil.org

• allinurl: Ten operator ogranicza wyniki do stron zawierających wszystkie zapytania podane w adresie URL. [allinurl: EC-Council career] - Zapytanie zwraca tylko strony zawierające w adresie URL słowa „EC-Council" i „career"

• inurl: Ten operator ogranicza wyniki do stron zawierających słowo określone w adresie URL. [inurl: copy site:www.eccouncil.org] - Zapytanie zwraca tylko te strony w witrynie EC-Council, których adres URL zawiera słowo „copy"

• allintitle: Ten operator ogranicza wyniki do stron zawierających wszystkie terminy zapytania określone w tytule. [allintitle: wykryj złośliwe oprogramowanie] - Zapytanie zwraca tylko strony zawierające w tytule słowa „wykryj" i „złośliwe oprogramowanie"

• inanchor: Ten operator ogranicza wyniki do stron zawierających warunki zapytania określone w tekście zakotwiczenia w linkach do strony. [Anti-virus inanchor:Norton] - Zapytanie zwraca tylko strony z tekstem zakotwiczenia w linkach do stron zawierających słowo „Norton" i strony zawierającej słowo „Antivirus"

• allinanchor: Ten operator ogranicza wyniki do stron zawierających wszystkie zapytania podane w tekście zakotwiczenia w linkach do strony. [allinanchor: najlepszy dostawca usług w chmurze] – Zapytanie zwraca tylko strony, na których tekst zakotwiczenia w linkach do stron zawiera słowa „najlepszy", „chmura", „usługa" i „dostawca"

• link: Ten operator przeszukuje strony internetowe lub strony, które zawierają linki do określonej witryny lub strony. [link:www.eccouncil.org] - wyszukuje strony wskazujące na stronę główną EC-Council

• related: Ten operator wyświetla strony internetowe, które są podobne lub powiązane z określonym adresem URL. [related:www.eccouncil.org] – Zapytanie udostępnia stronie wyników wyszukiwania Google strony internetowe podobne do eccouncil.org

• info: Ten operator wyszukuje informacje dla określonej strony internetowej.[info:eccouncil.org] - Zapytanie dostarcza informacji o lokalizacji strony głównej www.eccouncil.org

• location: Ten operator wyszukuje informacje dla określonej lokalizacji. [location: EC-Council] - zapytanie daje wyniki na podstawie terminu EC-Council.

11. Na tym kończy się demonstracja zbierania informacji przy użyciu zaawansowanych technik hakerskich Google. Korzystając z tych zaawansowanych operatorów Google, możesz samodzielnie przeprowadzić serię zapytań i zebrać odpowiednie informacje o docelowej organizacji.

12. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Zbierz informacje z wyszukiwarek wideo

Wyszukiwarki wideo to internetowe wyszukiwarki, które przeszukują sieć w poszukiwaniu treści wideo. Wyszukiwarki te zapewniają funkcję przesyłania i hostowania treści wideo na własnych serwerach internetowych lub mogą analizować treść wideo, która jest hostowana zewnętrznie. Tutaj przeprowadzimy zaawansowane wyszukiwanie wideo i odwrócone wyszukiwanie obrazów za pomocą wyszukiwarki YouTube i narzędzia YouTube Metadata.

Uwaga: W tym przypadku za organizację docelową uznamy EC-Council. Możesz jednak wybrać wybraną przez siebie organizację docelową.

1. Na maszynie wirtualnej Windows 11 uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.youtube.com i naciśnij Enter. Zostanie wyświetlona strona YouTube, jak pokazano na zrzucie ekranu.

Uwaga: jeśli zdecydujesz się użyć innej przeglądarki internetowej, zrzuty ekranu będą się różnić.

2. W polu wyszukiwania wyszukaj swoją organizację docelową (tutaj ec-council). Zobaczysz wszystkie najnowsze filmy przesłane przez organizację docelową.

3. Wybierz dowolny film, kliknij prawym przyciskiem myszy tytuł filmu i kliknij Kopiuj łącze.

4. Po skopiowaniu linku wideo otwórz nową kartę w przeglądarce Mozilla Firefox, umieść kursor myszy na pasku adresu, wpisz https://mattw.io/youtube-metadata/ i naciśnij Enter.

Uwaga: Aby otworzyć nową kartę, kliknij ikonę + obok pierwszej karty.

Uwaga: Narzędzie YouTube Metadata zbiera szczegółowe informacje o filmie, przesyłającym, liście odtwarzania oraz twórcy lub kanale.hare

5. Pojawi się strona Metadane YouTube, w polu Prześlij link do wyszukiwania filmu, listy odtwarzania lub kanału wklej skopiowaną lokalizację filmu YouTube i kliknij Prześlij.

6. Po zakończeniu wyszukiwania przewiń w dół i zobacz szczegóły związane z filmem, takie jak data i godzina publikacji, identyfikator kanału, tytuł itp. w sekcji Snippet.

7. Przewiń w dół, aby sprawdzić dodatkowe informacje w sekcjach Statystyki, Geolokalizacja, Status itp.

8. W sekcji Miniatura możesz znaleźć odwrócone wyniki wyszukiwania obrazu, kliknij przycisk Kliknij, aby odwrócić wyszukiwanie obrazu pod dowolną miniaturą.

9. Pojawi się nowa karta w Google i zostaną wyświetlone wyniki wyszukiwania wstecznego obrazu.

10. Na tym kończy się demonstracja zbierania informacji z zaawansowanego wyszukiwania wideo i odwrotnego wyszukiwania obrazu za pomocą wyszukiwarki YouTube i narzędzia YouTube Metadata.

11. Możesz korzystać z innych wyszukiwarek wideo, takich jak filmy Google (https://www.google.com/videohp), filmy Yahoo (https://in.video.search.yahoo.com) itp.; narzędzia do analizy wideo, takie jak EZGif (https://ezgif.com), VideoReverser.com (https://www.videoreverser.com) itp.; oraz narzędzia wyszukiwania wstecznego obrazu, takie jak TinEye Reverse Image Search (https://tineye.com), Yahoo Image Search (https://images.search.yahoo.com) itp. w celu zebrania kluczowych informacji o docelowej organizacji.

12. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 3: Zbierz informacje z wyszukiwarek FTP

Wyszukiwarki File Transfer Protocol (FTP) służą do wyszukiwania plików znajdujących się na serwerach FTP; pliki te mogą zawierać cenne informacje o docelowej organizacji. Wiele branż, instytucji, firm i uniwersytetów używa serwerów FTP do przechowywania dużych archiwów plików i innego oprogramowania, które są współużytkowane przez ich pracowników. Wyszukiwarki FTP dostarczają informacji o krytycznych plikach i katalogach, w tym cennych informacji, takich jak strategie biznesowe, dokumenty podatkowe, dane osobowe pracowników, dokumenty finansowe, licencjonowane oprogramowanie i inne poufne informacje. Flere, użyjemy indeksatora FTP NAPALM do wyszukiwania FTP w celu wyodrębnienia krytycznych informacji FTP o organizacji docelowej.

1. Na maszynie wirtualnej Windows 11 uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.searchftps.net/ i naciśnij Enter

Uwaga: jeśli zdecydujesz się użyć innej przeglądarki internetowej, zrzuty ekranu będą się różnić.

2. Pojawi się witryna indeksatora FTP NAPALM, jak pokazano na zrzucie ekranu.

3. W pasku wyszukiwania wpisz microsoft i kliknij Szukaj.

4. Otrzymasz wyniki wyszukiwania zawierające krytyczne pliki i dokumenty związane z organizacją docelową.

5. Na tym kończy się demonstracja zbierania informacji z wyszukiwarki FTP.

6. Możesz także użyć wyszukiwarek FTP, takich jak FreewareWeb FTP File Search (https://www.freewareweb.com), aby zebrać kluczowe informacje FTP o docelowej organizacji.

7. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

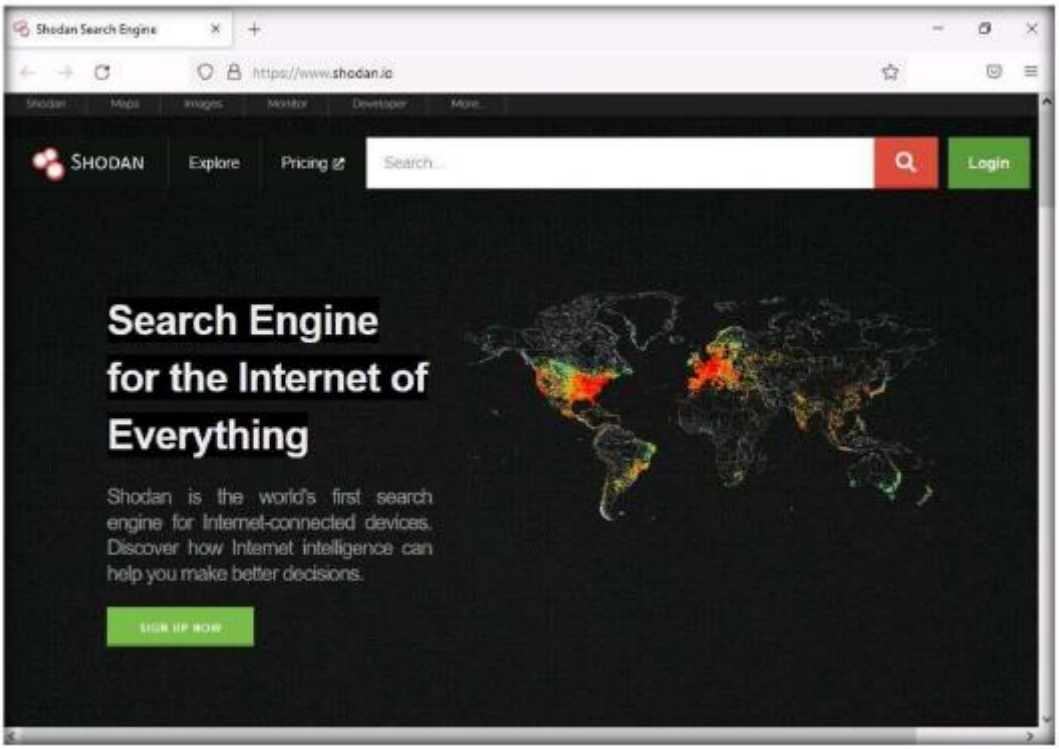
Zadanie 4: Zbierz informacje z wyszukiwarek IoT

Wyszukiwarki lot przeszukują Internet w poszukiwaniu publicznie dostępnych urządzeń IoT. Wyszukiwarki te dostarczają kluczowych informacji, w tym kontroli systemów SCADA (ang. w organizacji docelowej za pomocą wyszukiwarki Shodan IoT.

1. Na maszynie wirtualnej Windows 11 uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.shodan.io/ i naciśnij Enter.

Uwaga: jeśli zdecydujesz się użyć innej przeglądarki internetowej, zrzuty ekranu będą się różnić.

2. Pojawi się strona Shodan, jak pokazano na zrzucie ekranu.



3. W pasku wyszukiwania wpisz amazon i naciśnij Enter.

Uwaga: Tutaj szukamy publicznie dostępnych informacji na temat docelowej Amazon. Możesz jednak wyszukiwać według wybranego celu.

4. Otrzymasz wyniki wyszukiwania ze szczegółami wszystkich wrażliwych urządzeń IoT związanych z amazonem w różnych krajach.

5. Na tym kończy się demonstracja zbierania wrażliwych informacji IoT za pomocą wyszukiwarki Shodan.

6. Możesz także skorzystać z wyszukiwarki Censys (https://censys.io) IoT, aby zebrać informacje, takie jak dane producenta, położenie geograficzne, adres IP, nazwa hosta, otwarte porty itp.

7. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

8. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego. Wykonaj Footprinting za pośrednictwem usług sieciowych.

Usługi sieciowe to aplikacje lub źródła online, które dostarczają różnych publicznie dostępnych informacji związanych z organizacją docelową.

Scenariusz laboratoryjny

Jako zawodowy etyczny haker lub pen tester powinieneś być w stanie wydobyć z usług sieciowych różnorodne informacje o docelowej organizacji. W ten sposób możesz wyodrębnić krytyczne informacje, takie jak domeny docelowej organizacji, subdomeny, systemy operacyjne, lokalizacje geograficzne, dane pracowników, wiadomości e-mail, informacje finansowe, szczegóły infrastruktury,

ukryte strony internetowe i zawartość itp. Korzystając z tych informacji, możesz potrafi zbudować strategię hakerską, aby włamać się do sieci docelowej organizacji i przeprowadzić inne rodzaje zaawansowanych ataków systemowych.

Cele laboratorium

Znajdź domeny i subdomeny firmy za pomocą Netcraft

• Zbieraj dane osobowe za pomocą usługi wyszukiwania osób online PeekYou

• Zbierz listę e-mailową za pomocą Flarvester

• Zbieraj informacje, korzystając z głębokiego i ciemnego internetu

• Określ docelowy system operacyjny za pomocą pasywnego footprintingu

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

• Maszyna wirtualna Windows 11

• Maszyna wirtualna Parrot Security

• Przeglądarki internetowe z połączeniem internetowym

• Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 25 minut

Przegląd usług internetowych

Usługi sieciowe, takie jak portale społecznościowe, usługi wyszukiwania osób, usługi powiadamiania, usługi finansowe i witryny z ofertami pracy, dostarczają informacji o docelowej organizacji; na przykład szczegóły infrastruktury, lokalizacja fizyczna, dane pracowników itp. Ponadto grupy, fora i blogi mogą dostarczać poufnych informacji o organizacji docelowej, takich jak informacje o sieci publicznej, informacje o systemie i dane osobowe, archiwa internetowe mogą dostarczać poufnych informacji, które został usunięty z sieci World Wide Web (WWW).

Zadania laboratoryjne

Zadanie 1: Znajdź domeny i subdomeny firmy za pomocą Netcraft

Domeny i subdomeny są częścią krytycznej infrastruktury sieciowej każdej organizacji. Domeny najwyższego poziomu (TLD) i subdomeny firmy mogą dostarczać wielu przydatnych informacji, takich jak historia organizacji, usługi i produkty oraz dane kontaktowe. Ogólnodostępna strona internetowa ma na celu pokazanie obecności organizacji w Internecie i jest dostępna bezpłatnie. Tutaj wyodrębnimy domeny i subdomeny firmy za pomocą usługi sieciowej Netcraft.

1. Włącz maszynę wirtualną Windows 11.

2. Uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.netcraft.com i naciśnij Enter.

Uwaga: jeśli zdecydujesz się użyć innej przeglądarki internetowej, zrzuty ekranu będą się różnić.

3. Pojawi się strona Netcraft.

Uwaga: Jeśli w dolnej części przeglądarki pojawi się wyskakujące okienko cookie, kliknij Akceptuj.

4. Przejdź do Resources -> Tools -> Site Report.

5. Co działa ta witryna? pojawi się strona. Aby wyodrębnić informacje związane z witryną internetową organizacji, takie jak infrastruktura, używana technologia, subdomeny, tło, sieć itp., wpisz adres URL witryny docelowej (tutaj https://www.eccouncil.org) w polu tekstowym, a następnie kliknij przycisk Wyszukaj.

6. Zostanie wyświetlony raport witryny dla strony https://www.eccouncil.org, zawierający informacje dotyczące tła, sieci, historii hostingu itp.

7. W sekcji Sieć kliknij link do strony internetowej (tutaj eccouncil.org) w polu Domena, aby wyświetlić subdomeny.

8. Wynik wyświetli subdomeny docelowej witryny wraz z informacjami o blokadzie sieci i systemie operacyjnym.

9. Na tym kończy się demonstracja wyszukiwania domen i subdomen firmy za pomocą narzędzia Netcraft. Osoby atakujące mogą wykorzystać tę zebraną listę subdomen do przeprowadzania ataków aplikacji internetowych na organizację docelową, takich jak ataki polegające na wstrzykiwaniu, ataki brute-force i ataki typu „odmowa usługi" (DoS).

10. Możesz także użyć narzędzi takich jak Sublist3r (https://github.com), Pentest-Tools Find Subdomains (https://pentest-tools.com) itp., aby zidentyfikować domeny i subdomeny dowolnego celu strona internetowa.

11. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Zbierz dane osobowe za pomocą usługi PeekYou Online People Search

Usługi wyszukiwania osób online, zwane także witrynami z rejestrami publicznymi, są wykorzystywane przez wiele osób do znajdowania danych osobowych innych osób; usługi te dostarczają nazwisk, adresów, danych kontaktowych, daty urodzenia, zdjęć, filmów, zawodu, informacji o rodzinie i przyjaciołach, profilach w sieciach społecznościowych, informacjach o majątku i opcjonalnie przeszłości kryminalnej. Tutaj zbierzemy informacje o osobie z organizacji docelowej, przeprowadzając wyszukiwanie osób za pomocą internetowej usługi wyszukiwania osób PeekYou.

Uwaga: Tutaj zbieramy informacje o Satya Nadella z firmy Microsoft.

1. Na maszynie wirtualnej Windows 11 uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.peekyou.com i naciśnij Enter.

Uwaga: jeśli zdecydujesz się użyć innej przeglądarki internetowej, zrzuty ekranu będą się różnić.

2. Pojawi się strona PeekYou, jak pokazano na zrzucie ekranu.

Uwaga: Jeśli w dolnej części przeglądarki pojawi się wyskakujące okienko cookie, kliknij Zgadzam się.

4. Rozpocznie się wyszukiwanie osób i zostaną wyświetlone najlepsze dopasowania dla podanych parametrów wyszukiwania.

5. Wynik pokazuje informacje, takie jak rejestry publiczne, szczegóły tła, adresy e-mail, informacje kontaktowe, historia adresów itp. Te informacje pomagają atakującym w przeprowadzaniu phishingu, socjotechniki i innych rodzajów ataków.

6. Możesz dalej kliknąć hiperłącze Wyświetl pełny raport, aby wyświetlić szczegółowe informacje o osobie.

Uwaga: Po kliknięciu dowolnego wyniku zostaniesz przekierowany na inną stronę internetową, a załadowanie informacji o osobie zajmie trochę czasu.

7. Przewiń w dół, aby wyświetlić wszystkie informacje o osobie.

8. Na tym kończy się demonstracja zbierania danych osobowych za pomocą usługi wyszukiwania osób online PeekYou.

9. Możesz także użyć Spokeo (https://www.spokeo.com), pipl (https://pipl.com), Intelius (https://www.intelius.com), BeenVerified (https://www. .beenverified.com) itp., usługi wyszukiwania osób w celu zebrania danych osobowych kluczowych pracowników docelowej organizacji.

10. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 3: Zbierz listę e-mailową za pomocą narzędzia Harvester

Wiadomości e-mail to źródła wiadomości, które są kluczowe dla wymiany informacji. Identyfikator e-mail jest uważany przez większość ludzi za osobistą identyfikację pracowników lub organizacji. Dlatego gromadzenie identyfikatorów e-mail pracowników o krytycznym znaczeniu jest jednym z kluczowych zadań etycznych hakerów.

theHarvester: To narzędzie gromadzi wiadomości e-mail, subdomeny, hosty, nazwiska pracowników, otwarte porty i banery z różnych źródeł publicznych, takich jak wyszukiwarki, serwery kluczy PGP i komputerowa baza danych SHODAN, a także wykorzystuje Google, Bing, SHODAN itp. wydobyć cenne informacje z domeny docelowej. To narzędzie ma pomóc etycznym hakerom i testerom pióra na wczesnych etapach oceny bezpieczeństwa w zrozumieniu śladu organizacji w Internecie. Jest to również przydatne dla każdego, kto chce wiedzieć, jakie informacje organizacyjne są widoczne dla atakującego. Tutaj zbierzemy listę identyfikatorów e-mail związanych z organizacją docelową za pomocą narzędzia Harvester.

Uwaga: W tym przypadku za organizację docelową uznamy firmę Microsoft. Możesz jednak wybrać wybraną przez siebie organizację docelową.

1. Włącz maszynę wirtualną Parrot Security.

2. Na stronie logowania domyślnie zostanie wybrana nazwa użytkownika atakującego. Wprowadź hasło jako toor w polu Hasło i naciśnij Enter, aby zalogować się do urządzenia.

Uwaga: Jeśli wyskakujące okienko Parrot Updater pojawi się w prawym górnym rogu pulpitu, zignoruj je i zamknij.

Uwaga: Jeśli pojawi się wyskakujące okienko Pytanie z prośbą o aktualizację urządzenia, kliknij Nie, aby zamknąć okno.

3. Kliknij ikonę terminala MATE na górze pulpitu, aby otworzyć okno terminala.

4. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

5. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter.

Uwaga: Wpisane hasło nie będzie widoczne.

6. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

7. W oknie terminala wpisz Harvester -d microsoft.com -l 200 -b baidu i naciśnij Enter.

Uwaga: W tym poleceniu opcja -d określa domenę lub nazwę firmy do przeszukania, -l określa liczbę wyników do pobrania, a -b określa źródło danych.

8. theHarvester rozpoczyna wyodrębnianie szczegółów i wyświetla je na ekranie.

9. Możesz zobaczyć identyfikatory e-mail powiązane z firmą docelową i hostami firmy docelowej uzyskane ze źródła Baidu, jak pokazano na zrzucie ekranu. Osoby atakujące mogą wykorzystywać te listy e-mail i nazwy użytkowników do przeprowadzania ataków socjotechnicznych i ataków siłowych na atakowaną organizację.

Uwaga: Podczas wykonywania tego zadania wyniki mogą się różnić.

Uwaga: Tutaj jako źródło danych określamy wyszukiwarkę Baidu. Możesz określić różne źródła danych (np. Baidu, bing, binaryedge, bingapi, censys, google, linkedin, twitter, virustotal, ThreatCrowd, crtsh, netcraft, yahoo itp.), aby zebrać informacje o celu.

10. Na tym kończy się demonstracja zbierania listy e-mailowej za pomocą narzędzia Harvester.

11. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

12. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 4: Zbierz informacje za pomocą wyszukiwania w Deep i Dark Web

Głęboka sieć składa się ze stron internetowych i treści, które są ukryte i niezindeksowane i których nie można zlokalizować za pomocą tradycyjnej przeglądarki internetowej i wyszukiwarek. Dostęp do niej można uzyskać za pomocą wyszukiwarek, takich jak przeglądarka Tor i wirtualna biblioteka WWW. Ciemna sieć lub ciemna sieć to podzbiór głębokiej sieci, w której każdy może poruszać się anonimowo bez śledzenia. Wyszukiwanie w głębokiej i ciemnej sieci może dostarczyć krytycznych informacji, takich jak dane karty kredytowej, dane paszportowe, dane dowodu osobistego, dokumentacja medyczna, konta w mediach społecznościowych, numery ubezpieczenia społecznego (SSN) itp. W tym miejscu zrozumiemy różnicę między wyszukiwaniem w sieci powierzchniowej a wyszukiwanie w ciemnej sieci przy użyciu przeglądarki Mozilla Firefox i Tor Browser.

1. Przełącz się na maszynę wirtualną Windows 11. Zaloguj się do maszyny wirtualnej Windows 11 za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd.

2. Otwórz Eksplorator plików, przejdź do C:\Users\Admin\Desktop\Tor Browser i kliknij dwukrotnie

Uruchom przeglądarkę Tor.

3. Pojawi się strona Połącz z Tor. Kliknij przycisk Połącz, aby bezpośrednio przeglądać domyślne ustawienia przeglądarki Tor.

Uwaga: Jeśli Tor jest ocenzurowany w twoim kraju lub jeśli chcesz połączyć się przez serwer proxy, kliknij przycisk Ustawienia sieci Tor i kontynuuj.

4. Po kilku sekundach pojawi się strona główna przeglądarki Tor. Główną zaletą przeglądarki Tor Browser jest zachowanie anonimowości użytkownika podczas całej sesji.

5. Jako etyczny haker musisz zebrać wszystkie możliwe informacje dotyczące organizacji docelowej z ciemnej sieci. Zanim to zrobisz, musisz znać różnicę między wyszukiwaniem w sieci powierzchniowej a wyszukiwaniem w ciemnej sieci.

6. Aby zrozumieć wyszukiwanie w sieci na powierzchni, najpierw zminimalizuj przeglądarkę Tor i otwórz Mozilla Firefox. Przejdź do www.google.com; w pasku wyszukiwania Google wyszukaj informacje związane z hakerem do wynajęcia. Zostanie wyświetlonych wiele nieistotnych danych, jak pokazano na zrzucie ekranu.

7. Teraz przełącz się do przeglądarki Tor i wyszukaj to samo (tj. hakera do wynajęcia). Znajdziesz odpowiednie linki związane z profesjonalnymi hakerami, którzy działają pod ziemią poprzez ciemną sieć.

Uwaga: Tor używa wyszukiwarki DuckDuckGo do wyszukiwania w ciemnej sieci. Wyniki mogą się różnić w twoim środowisku.

8. Domyślnie wybrany jest parametr wyszukiwania we wszystkich regionach. Możesz jednak kliknąć strzałkę w dół, aby wyświetlić opcje rozwijane i wybrać wybrany region, który określa kraj VPN/Proxy.

9. Wyniki wyszukiwania hakera do wynajęcia zostaną załadowane. Kliknij, aby otworzyć dowolną witrynę z wyników wyszukiwania (tutaj https://www.hackerforhire.net).

Uwaga: Podczas wykonywania tego zadania wyniki wyszukiwania mogą się różnić.

10. Otworzy się strona internetowa https://www.hackerforhire.net Widać, że strona należy do profesjonalnych hakerów, którzy działają w podziemiu.

11. Hackerforhire to przykład. Te wyniki wyszukiwania pomogą Ci zidentyfikować profesjonalnych hakerów. Jednak jako etyczny haker możesz zbierać krytyczne i poufne informacje o swojej docelowej organizacji, korzystając z wyszukiwania w głębokiej i ciemnej sieci.

12. Możesz także anonimowo eksplorować następujące strony z cebulą za pomocą Tor Brower w celu zebrania innych istotnych informacji o docelowej organizacji:

* The Hidden Wiki to strona cebulowa, która działa jako usługa Wikipedii dla ukrytych stron internetowych.

(http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki)

* FakeID to strona cebulowa do tworzenia fałszywych paszportów

(http://ymvhtqya23wqpez63gyc3ke4svju3mqsby2awnhd3bk2e65izt7baqad.onion)

* Cardshop to strona z cebulą, która sprzedaje karty z dobrym saldem

(http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion)

13. Możesz także użyć narzędzi, takich jak ExoneraTor (https://metrics.torproject.org), OnionLand Search engine (https://onionlandsearchengine.com) itp., aby przeglądać głębokie i ciemne strony internetowe.

14. To kończy demonstrację zbierania informacji za pomocą głębokiego i ciemnego wyszukiwania w sieci za pomocą przeglądarki Tor.

15. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 5: Określ docelowy system operacyjny za pomocą pasywnego footprintingu

Informacje o systemie operacyjnym są kluczowe dla każdego etycznego hakera. Etyczni hakerzy mogą uzyskać szczegółowe informacje na temat systemu operacyjnego działającego na docelowej maszynie, wykonując różne pasywne techniki śledzenia i uzyskując inne informacje, takie jak miasto, kraj, szerokość/długość geograficzna, nazwa hosta, system operacyjny i adres IP docelowej organizacji. Tutaj zbierzemy informacje o docelowym systemie operacyjnym poprzez pasywne śledzenie za pomocą usługi internetowej Censys.

Uwaga: W tym przypadku za organizację docelową uznamy EC-Council. Możesz jednak wybrać wybraną przez siebie organizację docelową.

1. Na maszynie wirtualnej Windows 11 uruchom dowolną przeglądarkę, w tym laboratorium używamy Mozilla Firefox. W pasku adresu przeglądarki umieść kursor myszy i wpisz https://search.censys.io/?q= i naciśnij Enter.

2. W polu wyszukiwania wpisz docelową stronę internetową (tutaj www.eccouncil.org) i naciśnij Enter. W wynikach kliknij dowolny adres IP hosta, dla którego chcesz zebrać szczegóły systemu operacyjnego.

Uwaga: Wynik może się różnić w przypadku wykonania tego zadania laboratoryjnego.

3. Zostanie wyświetlona wybrana strona hosta. W sekcji Informacje podstawowe możesz zauważyć, że system operacyjny to Ubuntu. Oprócz tego można również obserwować inne szczegóły, takie jak uruchomione protokoły, oprogramowanie, klucze hosta itp. Informacje te mogą pomóc atakującym w zidentyfikowaniu potencjalnych luk i znalezieniu skutecznych exploitów do przeprowadzenia różnych ataków na atakowaną organizację.

4. Na tym kończy się demonstracja zbierania informacji o systemie operacyjnym poprzez pasywny footprinting za pomocą usługi sieciowej Censys.

5. Możesz także korzystać z usług internetowych, takich jak Netcraft (https://www.netcraft.com), Shodan (https://www.shodan.io) itp., aby zbierać informacje o systemie operacyjnym docelowej organizacji poprzez pasywne śledzenie.

6. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

7. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj Footprinting za pośrednictwem serwisów społecznościowych

Serwisy społecznościowe to usługi, platformy lub strony internetowe, które koncentrują się na ułatwianiu budowania sieci społecznościowych lub relacji społecznych między ludźmi.

Scenariusz laboratoryjny

Jako profesjonalny etyczny haker podczas zbierania informacji musisz zbierać dane osobowe pracowników pracujących na krytycznych stanowiskach w docelowej organizacji; na przykład główny specjalista ds. bezpieczeństwa informacji, architekt bezpieczeństwa lub administrator sieci. Śledząc ślady za pośrednictwem serwisów społecznościowych, można wyodrębnić dane osobowe, takie jak imię i nazwisko, stanowisko, nazwę organizacji, aktualną lokalizację i kwalifikacje edukacyjne. Ponadto

możesz znaleźć profesjonalne informacje, takie jak firma, aktualna lokalizacja, numer telefonu, identyfikator e-mail, zdjęcia, filmy itp. Zebrane informacje mogą być przydatne do przeprowadzania inżynierii społecznej i innych rodzajów zaawansowanych ataków.

Cele laboratorium

* Zbieraj informacje o pracownikach z Linkedln za pomocą narzędzia Harvester

* Zbieraj dane osobowe z różnych serwisów społecznościowych za pomocą Sherlocka

* Zbieraj informacje za pomocą Followerwonk

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Maszyna wirtualna Parrot Security

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 15 minut

Przegląd serwisów społecznościowych

Serwisy społecznościowe to usługi, platformy lub inne witryny internetowe, które umożliwiają ludziom łączenie się i budowanie relacji międzyludzkich. Ludzie zwykle prowadzą profile w serwisach społecznościowych, aby dostarczać podstawowych informacji o sobie oraz pomagać w nawiązywaniu i utrzymywaniu kontaktów z innymi; profil zazwyczaj zawiera informacje, takie jak imię i nazwisko, dane kontaktowe (numer telefonu komórkowego, adres e-mail), informacje o znajomych, informacje o członkach rodziny, ich zainteresowaniach, działaniach itp. Na portalach społecznościowych ludzie mogą również umieszczać swoje dane osobowe, takie jak data urodzenia, informacje o wykształceniu, doświadczenie zawodowe, imiona współmałżonków itp. Organizacje często publikują informacje, takie jak potencjalni partnerzy, strony internetowe i nadchodzące wiadomości o firmie. Tym samym portale społecznościowe często okazują się cennym źródłem informacji. Przykładami takich witryn są Linkedln, Facebook, Instagram, Twitter, Pinterest, YouTube itp.

Zadania laboratoryjne

Zadanie 1: Zbierz informacje o pracownikach z Linkedln za pomocą narzędzia Harvester

Linkedln to portal społecznościowy dla profesjonalistów z branży. Łączy światowe zasoby ludzkie, aby wspierać produktywność i sukces. Witryna zawiera dane osobowe, takie jak imię i nazwisko, stanowisko, nazwę organizacji, aktualną lokalizację, wykształcenie itp. Flere, będziemy gromadzić informacje o pracownikach (nazwisko i stanowisko) organizacji docelowej, które są dostępne na Linkedln za pomocą narzędzia theHarvester.

Uwaga: W tym przypadku za organizację docelową uznamy Radę WE. Możesz jednak wybrać wybraną przez siebie organizację docelową.

1. Włącz maszynę wirtualną Parrot Security. Na stronie logowania domyślnie zostanie wybrana nazwa użytkownika atakującego. Wprowadź hasło jako toor w polu Hasło i naciśnij Enter, aby zalogować się do urządzenia.

2. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

3. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

4. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

5. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

6. W oknie terminala wpisz theHarvester -d eccouncil -l 200 -b linkedin i naciśnij Enter, aby zobaczyć 200 wyników EC-Council ze źródła Linkedin.

Uwaga: W tym poleceniu -d określa domenę lub nazwę firmy do przeszukania (tutaj eccouncil), -l określa liczbę wyników do pobrania, a -b określa źródło danych jako Linkedin.

Uwaga: Cała domena eccouncil to eccouncil.org.

7. Przewiń w dół, aby wyświetlić listę pracowników wraz z ich rolami w EC-Council. Te informacje z LinkedIn mogą pomóc atakującym w przeprowadzaniu ataków socjotechnicznych lub phishingowych.

8. Na tym kończy się demonstracja zbierania informacji o pracownikach z serwisu Linkedin za pomocą narzędzia Harvester.

9. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Zbierz dane osobowe z różnych serwisów społecznościowych za pomocą Sherlocka

Sherlock to narzędzie oparte na Pythonie, które służy do zbierania informacji o osobie docelowej za pośrednictwem różnych serwisów społecznościowych. Sherlock przeszukuje ogromną liczbę serwisów społecznościowych dla danego użytkownika docelowego, lokalizuje tę osobę i wyświetla wyniki wraz z pełnym adresem URL związanym z osobą docelową. Tutaj użyjemy Sherlocka do zebrania danych osobowych o celu z portali społecznościowych.

Uwaga: Tutaj zbieramy informacje o Satyi Nadelli. Możesz jednak wybrać cel według własnego uznania.

1. W maszynie wirtualnej Parrot Security kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

2. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

3. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

4. Wpisz cd sherlock/sherlock/ i naciśnij Enter, aby przejść do folderu Sherlock.

5. Wpisz python3 sherlock.py satya nadella i naciśnij Enter. Otrzymasz wszystkie adresy URL związane z Satyą Nadellą, jak pokazano na zrzucie ekranu. Przewiń w dół, aby wyświetlić wszystkie wyniki.

Uwaga: Podczas wykonywania tego zadania wyniki mogą się różnić. Jeśli w międzyczasie pojawią się komunikaty o błędach, zignoruj je.

6. Atakujący mogą następnie wykorzystać zebrane adresy URL do uzyskania poufnych informacji o celu, takich jak data urodzenia, status zatrudnienia i informacje o organizacji, dla której pracują, w tym strategia biznesowa, potencjalni klienci i plany nadchodzących projektów.

7. Na tym kończy się demonstracja zbierania informacji o osobach z różnych serwisów społecznościowych za pomocą Sherlocka.

8. Możesz także skorzystać z narzędzi takich jak Social Searcher (https://www.social-searcher.com), UserRecon (https://github.com) itp., aby zebrać dodatkowe informacje dotyczące firmy docelowej i jej pracowników z serwisów społecznościowych.

9. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

10. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 3: Zbierz informacje za pomocą Followerwonka

Followerwonk to narzędzie online, które pomaga odkrywać i rozwijać wykres społecznościowy, zagłębiając się w statystyki Twittera; na przykład Kim są twoi followersi? Gdzie się znajdują? Kiedy tweetują? Można to wykorzystać do zebrania informacji z Twittera o dowolnej docelowej organizacji lub osobie. Tutaj użyjemy Followerwonk do zbierania informacji o obserwujących w serwisach społecznościowych.

1. Włącz maszynę wirtualną Windows 11. Zaloguj się do maszyny wirtualnej Windows 11 za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd.

2. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy, wpisz https://followerwonk.com/analyze i naciśnij Enter.

3. Pojawi się strona Followerwonk.

4. W pasku wyszukiwania nazwy ekranowej wpisz tag twitter osoby docelowej (tutaj @satyanadella) i kliknij przycisk Zrób to, aby przeanalizować użytkowników, których obserwuje osoba docelowa.

5. Pojawią się wyniki dotyczące celu.

6. Przewiń w dół, aby wyświetlić szczegółową analizę położenia geograficznego i godzin aktywności obserwujących. Te informacje dodatkowo pomagają atakującym w przeprowadzaniu różnych ataków socjotechnicznych i nietechnicznych.

7. To kończy demonstrację zbierania informacji za pomocą Followerwonk.

8. Możesz także skorzystać z Hootsuite (https://www.hootsuite.com), Meltwater (https://www.meltwater.com) itp. w celu zebrania dodatkowych informacji związanych z firmą docelową i jej pracownikami z portali społecznościowych .

9. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

10. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj Footprinting witryny

Footprinting witryny internetowej odnosi się do monitorowania i analizowania strony internetowej organizacji docelowej w celu uzyskania informacji.

Scenariusz laboratoryjny

Jako zawodowy etyczny haker powinieneś być w stanie wydobyć różne informacje o docelowej organizacji z jej strony internetowej; wykonując footprinting witryny, możesz wydobyć ważne informacje związane z witryną docelowej organizacji, takie jak używane oprogramowanie i jego wersja, szczegóły systemu operacyjnego, nazwy plików, ścieżki, nazwy pól bazy danych, dane kontaktowe, dane CMS, technologia zastosowana do budowy witryny , platformę skryptową itp. Korzystając z tych informacji, możesz dalej planować przeprowadzenie zaawansowanych ataków na organizację docelową.

Cele laboratorium

• Zbierz informacje o docelowej witrynie za pomocą narzędzia wiersza poleceń ping

• Zbierz informacje o docelowej stronie za pomocą Photona

• Zbierz informacje o docelowej witrynie za pomocą Central Ops

• Wyodrębnij dane firmy za pomocą narzędzia Web Data Extractor

• Kopiuj docelową witrynę za pomocą HTTrack Web Site Copier

• Zbierz informacje o docelowej stronie internetowej za pomocą GRecon

• Zbierz listę słów z docelowej strony internetowej za pomocą CeWL

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

• Maszyna wirtualna Windows 11

• Maszyna wirtualna Parrot Security

• Przeglądarki internetowe z połączeniem internetowym

• Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 45 minut

Przegląd Footprintingu witryny

Footprinting witryny to technika wykorzystywana do zbierania informacji dotyczących witryny docelowej organizacji. Śledzenie witryny może dostarczyć poufnych informacji związanych z witryną, takich jak zarejestrowane nazwy i adresy właściciela domeny, nazwy domen, host witryn, szczegóły systemu operacyjnego, dane IP, dane rejestratora, adresy e-mail, nazwy plików itp.

Zadania laboratoryjne

Zadanie 1: Zbierz informacje o witrynie docelowej za pomocą narzędzia wiersza poleceń Ping

Ping to narzędzie do administrowania siecią używane do testowania osiągalności hosta w sieci IP i mierzenia czasu obiegu wiadomości wysyłanych z hosta źródłowego do komputera docelowego.

Polecenie ping wysyła żądanie echa ICMP do hosta docelowego i czeka na odpowiedź ICMP. Podczas tego procesu żądanie-odpowiedź polecenie ping mierzy czas od wysłania do odbioru, zwany czasem podróży w obie strony, i rejestruje utratę pakietów. Polecenie ping pomaga w uzyskaniu informacji o domenie i adresie IP docelowej strony internetowej. Tutaj użyjemy narzędzia wiersza poleceń ping do zebrania informacji o docelowej witrynie.

1. Włącz maszynę wirtualną Windows 11. Zaloguj się do maszyny wirtualnej Windows 11 za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd.

2. Otwórz okno wiersza polecenia. Wpisz ping www.certifiedhacker.com i naciśnij Enter, aby znaleźć jego adres IP.

Uwaga: Aby otworzyć okno wiersza polecenia, kliknij ikonę Szukaj na pulpicie, wpisz cmd i wybierz z wyników Wiersz polecenia.

3. Zanotuj adres IP domeny docelowej w powyższym wyniku (tutaj 162.241.216.11). Otrzymujesz również informacje na temat statystyk Ping, takie jak wysłane pakiety, odebrane pakiety, utracone pakiety i przybliżony czas podróży w obie strony.

4. W oknie wiersza polecenia wpisz ping www.certifiedhacker.com -f -l 1500 i naciśnij Enter.

Uwaga: Tutaj, -f: Określa ustawienie flagi braku fragmentacji w pakiecie, -l: Określa rozmiar bufora.

5. Odpowiedź „Pakiet musi być pofragmentowany, ale DF ustawiony" oznacza, że ramka jest za duża, aby mogła znaleźć się w sieci i musi zostać pofragmentowana. Pakiet nie został wysłany, ponieważ użyliśmy przełącznika -f z poleceniem ping, a polecenie ping zwróciło ten błąd.

6. W oknie wiersza polecenia wpisz ping www.certifiedhacker.com -f -l 1300 i naciśnij Enter.

7. Zwróć uwagę, że maksymalny rozmiar pakietu jest mniejszy niż 1500 bajtów i większy niż 1300 bajtów.

8. Teraz wypróbuj różne wartości, aż znajdziesz maksymalny rozmiar klatki. Na przykład ping www.certifiedhacker.com -f -11473 odpowiada pakietem, który musi być pofragmentowany, ale ustawiony jest DF, a ping www.certifiedhacker.com -f -l 1472 odpowiada pomyślnym pingiem. Wskazuje, że 1472 bajty to maksymalny rozmiar ramki w sieci tego komputera.

9. Teraz odkryj, co się stanie, gdy TTL (Time to Live) wygaśnie. Każda ramka w sieci ma zdefiniowany TTL. Jeśli TTL osiągnie 0, router odrzuca pakiet. Mechanizm ten zapobiega utracie pakietów.

10. W oknie wiersza polecenia wpisz ping www.certifiedhacker.com -i 3 i naciśnij Enter. Ta opcja ustawia wartość czasu życia (-i) na 3.

Uwaga: Maksymalna wartość, jaką można ustawić dla TTL, to 255.

11. Odpowiedź z 192.168.100.6: TTL wygasł podczas przesyłania oznacza, że router (192.168.100.6, będziesz miał inny adres IP) odrzucił ramkę, ponieważ jego TTL wygasł (osiągnął 0).

Uwaga: Adres IP 192.168.100.6 może się zmienić podczas wykonywania tego zadania.

12. Zminimalizuj wiersz polecenia pokazany powyżej i uruchom nowy wiersz polecenia. Wpisz ping www.certifiedhacker.com -i 2 -n 1 i naciśnij Enter. Tutaj ustawiamy wartość TTL na 2, a wartość -n na 1, aby sprawdzić żywotność pakietu.

Uwaga: -n określa liczbę żądań echa, które mają zostać wysłane do celu.

13. Wpisz ping www.certifiedhacker.com -i 3 -n 1. Spowoduje to ustawienie wartości TTL na 3.

14. Zauważ, że odpowiedź pochodzi z adresu IP 162.241.216.11 i nie ma utraty pakietów.

15. Teraz zmień wartość czasu życia na 4, wpisując polecenie ping www.certifiedhacker.com -i 4 –n 1i naciśnij Enter.

16. Powtarzaj powyższy krok, aż uzyskasz adres IP www.certifiedhacker.com (w tym przypadku 162.241.216.11).

17. Znajdź wartość przeskoku, próbując różnych wartości TTL, aby uzyskać dostęp do www.certifiedhacker.com.

Uwaga: W tym przypadku wartość nadziei na dotarcie do www.certifiedhacker.com wynosi 19, co może się różnić podczas wykonywania tego zadania.

18. Pomyślne znalezienie wartości TTL będzie oznaczać, że otrzymano odpowiedź z hosta docelowego (162.241.216.11).

19. To kończy demonstrację zbierania informacji o docelowej witrynie za pomocą narzędzia wiersza poleceń Ping (takich jak adres IP docelowej witryny, liczba przeskoków do celu oraz wartość maksymalnego dozwolonego rozmiaru ramki w sieci docelowej).

20. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Zbierz informacje o docelowej witrynie za pomocą Photona

Photon to skrypt Pythona używany do indeksowania określonego docelowego adresu URL w celu uzyskania informacji, takich jak adresy URL (w zakresie i poza zakresem), adresy URL z parametrami, adresy e-mail, konta w mediach społecznościowych, pliki, tajne klucze i subdomeny. Wyodrębnione informacje można dalej eksportować w formacie JSON.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Włącz maszynę wirtualną Parrot Security.

2. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

3. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

4. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

5. W oknie terminala wpisz cd Photon i naciśnij Enter, aby przejść do repozytorium Photon.

6. Wpisz python3 photon.py -h i naciśnij Enter, aby wyświetlić listę opcji udostępnianych przez Photon.

7. Wpisz python3 photon.py -u http://www.certifiedhacker.com i naciśnij Enter, aby zaindeksować docelową witrynę pod kątem adresów URL wewnętrznych, zewnętrznych i skryptów.

Uwaga: -u: określa docelową stronę internetową (tutaj www.certifiedhacker.com).

8. Uzyskane wyniki zapisywane są w katalogu www.certifiedhacker.com w folderze Photon.

Uwaga: Dane wyjściowe mogą się różnić podczas wykonywania tego zadania.

9. Wpisz Is i naciśnij Enter, aby wyświetlić zawartość folderu.

10. Możesz zauważyć, że tworzony jest katalog o nazwie www.certifiedhacker.com.

11. Teraz kliknij Miejsca w górnej części pulpitu i wybierz Folder domowy.

12. Pojawi się okno atakującego, przejdź do folderu Photon --> www.certifiedhacker.com.

13. W tym folderze możesz obserwować trzy pliki tekstowe: zewnętrzny, wewnętrzny i skrypty.

14. Kliknij dwukrotnie plik external.txt, aby wyświetlić zawartość pliku.

15. Pojawi się okno edytora tekstu Pluma pokazujące zewnętrzne adresy URL uzyskane za pomocą Photona.

Uwaga: Dane wyjściowe mogą się różnić podczas wykonywania zadania.

16. Podobnie możesz przeglądać wewnętrzne i skryptowe pliki tekstowe zawierające adresy URL indeksowane przez narzędzie Photon.

17. Zamknij okno edytora tekstu Pluma i przełącz się z powrotem do okna Terminala.

18. Teraz wpisz python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 - wayback i naciśnij Enter, aby zaindeksować witrynę docelową przy użyciu adresów URL z archive.org.

Notatka:

• -u: określa docelową stronę internetową (tutaj www.certifiedhacker.com)

• -l: określa poziom indeksowania (tutaj 3)

• -t: określa liczbę wątków (tutaj 200)

• -wayback: określa użycie adresów URL z archive.org jako nasion

Uwaga: Dane wyjściowe mogą się różnić podczas wykonywania zadania.

19. Uzyskane wyniki zapisywane są w katalogu www.certifiedhacker.com w folderze Photon. Możesz przejść do folderu www.certifiedhacker.com, aby wyświetlić wynik.

20. Możesz dalej eksplorować narzędzie Photon i wykonywać różne inne funkcje, takie jak klonowanie docelowej witryny, wydobywanie tajnych kluczy i plików cookie, uzyskiwanie ciągów znaków poprzez określenie wzorca wyrażenia regularnego itp. Korzystając z tych informacji, osoby atakujące mogą przeprowadzać różne ataki na witryna docelowa, takie jak ataki brute-force, ataki typu „odmowa usługi", ataki typu „wstrzyknięcie", ataki typu „phishing" i ataki socjotechniczne.

21. Na tym kończy się demonstracja zbierania informacji na docelowym serwisie za pomocą narzędzia Photon.

22. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

23. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 3: Zbierz informacje o witrynie docelowej za pomocą Central Ops

CentralOps (centralops.net) to darmowy skaner sieci online, który bada domeny i adresy IP, rekordy DNS, traceroute, nslookup, wyszukiwania whois itp.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Przełącz się na maszynę wirtualną Windows 11. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy, wpisz https://centralops.net i naciśnij Enter. Witryna Central Ops pojawia się

2. Aby wyodrębnić informacje powiązane z witryną organizacji docelowej, wpisz adres URL docelowej witryny (tutaj www.certifiedhacker.com) w polu wprowadź domenę lub adres IP, a następnie kliknij przycisk Przejdź.

3. Wynik wyszukiwania WWW.CERTIFIEDHACKER.COM zawierający informacje takie jak wyszukiwanie adresu, rekord Domain Whois.

4. Przewiń w dół, aby wyświetlić informacje, takie jak rekord sieci Whois i rekordy DNS. Atakujący mogą wykorzystać te informacje do wykonania iniekcji i innych ataków aplikacji internetowych na docelową stronę internetową.

5. To kończy demonstrację zbierania informacji o docelowej stronie internetowej za pomocą internetowego narzędzia Central Ops.

6. Możesz także skorzystać z narzędzi takich jak Website Informer (https://website.informer.com), Burp Suite (https://portswigger.net), Zaproxy (https://www.zaproxy.org) itp. w celu wykonania śledzenia strony internetowej na docelowej stronie internetowej.

7. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 4: Wyodrębnij dane firmy za pomocą narzędzia Web Data Extractor

Ekstrakcja danych internetowych to proces wydobywania danych ze stron internetowych dostępnych na stronie internetowej firmy. Dane firmy, takie jak dane kontaktowe (adres e-mail, numer telefonu i faks), adresy URL, metatagi (tytuł, opis, słowo kluczowe) do promocji witryny, katalogi, badania sieci itp. są ważnym źródłem informacji dla etycznego hakera. Pająki internetowe (znane również jako roboty indeksujące lub roboty internetowe), takie jak Web Data Extractor, wykonują automatyczne wyszukiwania w witrynie docelowej i wydobywają określone informacje z witryny docelowej. Tutaj zbierzemy dane firmy docelowej za pomocą narzędzia Web Data Extractor.

1. Na komputerze z systemem Windows 11 przejdź http://www.webextractor.com/.

Uwaga: Jeśli pojawi się wyskakujące okienko Ostrzeżenie o zabezpieczeniach otwartego pliku, kliknij Uruchom.

2. Pobierz plik i zainstaluj .

3. Postępuj zgodnie z instrukcjami kreatora, aby zainstalować narzędzie Web Data Extractor i kliknij przycisk Zakończ.

4. Kliknij ikonę wyszukiwania ( ) na pulpicie i wpisz dane internetowe w polu wyszukiwania. W wynikach pojawi się Web Data Extractor, kliknij Open, aby go uruchomić.

5. Pojawi się okno główne Web Data Extractor. Kliknij Nowy, aby rozpocząć nową sesję.

6. Pojawi się okno Ustawienia sesji; wpisz adres URL (tutaj http://www.certifiedhacker.com) w polu Początkowy adres URL. Zaznacz wszystkie opcje i kliknij OK.

7. Kliknij Start, aby rozpocząć ekstrakcję danych.

8. Web Data Extractor rozpocznie zbieranie informacji (sesja, metatagi, e-maile, telefony, faksy, scalona lista, adresy URL i nieaktywne witryny).

9. Po zakończeniu procesu ekstrakcji danych pojawi się okno dialogowe Informacje; Kliknij OK.

Uwaga: Wyniki mogą się różnić w zależności od wykonania zadania.

10. Wyświetl wyodrębnione informacje, klikając karty.

11. Wybierz kartę Metatagi, aby wyświetlić adres URL, tytuł, słowa kluczowe, opis, hosta, domenę, rozmiar strony itp.

12. Wybierz kartę Wiadomości e-mail, aby wyświetlić informacje związane z wiadomościami e-mail, takie jak adres e-mail, nazwa, adres URL, tytuł itp.

13. Wybierz kartę Telefony, aby wyświetlić telefon, źródło, znacznik, adres URL itp.

14. Sprawdź więcej informacji na kartach Faksy, Scalona lista, Adresy URL i Nieaktywne strony.

15. Aby zapisać sesję, wybierz Plik i kliknij Zapisz sesję.

16. Określ nazwę sesji (tutaj: Certifiedhacker.com) w oknie dialogowym Zapisz sesję i kliknij OK.

17. Kliknij kartę Metatagi, a następnie kliknij ikonę dyskietki.

18. Może pojawić się wyskakujące okienko informacyjne z komunikatem Nie można zapisać więcej niż 10 rekordów w wersji demonstracyjnej; Kliknij OK.

19. Pojawi się okno Zapisz metatagi. W polu Nazwa pliku kliknij ikonę folderu, wybierz lokalizację, w której chcesz zapisać plik, wybierz Format pliku i kliknij Zapisz. Zebrane informacje mogą zostać wykorzystane przez osoby atakujące do przeprowadzania ataków, takich jak socjotechnika i ataki na aplikacje internetowe na docelowej stronie internetowej.

20. Domyślnie sesja zostanie zapisana w C:\Program Files(x86)\WebExtractor\Data\certifiedhacker.com. Możesz wybrać żądaną lokalizację, aby zapisać plik.

21. Na tym kończy się demonstracja wyodrębniania danych firmy za pomocą narzędzia Web Data Extractor.

22. Możesz także użyć innych pająków sieciowych, takich jak ParseHub (https://www.parsehub.com), SpiderFoot (https://www.spiderfoot.net) itp., aby wyodrębnić dane docelowej organizacji.

23. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 5: Wykonaj kopię lustrzaną witryny docelowej za pomocą HTTrack Web Site Copier

Dublowanie witryn internetowych to proces tworzenia repliki lub klonu oryginalnej witryny internetowej; kopia lustrzana witryny internetowej pomaga w dokładnym rozmieszczeniu witryny internetowej w systemie lokalnym i umożliwia pobranie witryny internetowej do lokalnego katalogu, analizę wszystkich katalogów, kodu HTML, obrazów, plików flash, filmów i innych plików z serwera na komputerze użytkownika komputer. Możesz powielać strony internetowe za pomocą narzędzi do tworzenia kopii lustrzanych stron internetowych, takich jak HTTrack Web Site Copier. HTTrack to narzędzie przeglądarki działające w trybie offline, które pobiera witrynę internetową z Internetu do lokalnego katalogu, rekurencyjnie buduje wszystkie katalogi i przesyła kod HTML, obrazy i inne pliki z serwera WWW na inny komputer. W tym przypadku użyjemy narzędzia HTTrack Web Site Copier do

odzwierciedlenia całej witryny docelowej organizacji, zapisania jej na lokalnym dysku systemowym i przeglądania lokalnej witryny w celu zidentyfikowania możliwych exploitów i luk w zabezpieczeniach.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Na maszynie wirtualnej Windows 11 kliknij ikonę Szukaj na pulpicie i wpisz winhttrack w polu wyszukiwania. W wynikach pojawi się narzędzie WinHTTrack Website Copier. Kliknij Otwórz, aby je uruchomić.

2. Pojawi się okno O WinHTTrack Website Copier. Kliknij OK w wyskakującym oknie, a następnie kliknij Dalej >, aby utworzyć nowy projekt.

3. Wprowadź nazwę projektu (tutaj Projekt testowy) w polu Nowa nazwa projektu:. Wybierz ścieżkę podstawową: do przechowywania skopiowanych plików; kliknij Dalej >.

4. Wprowadź docelowy adres URL (tutaj www.certifiedhacker.com) w polu Adresy internetowe: (URL) i kliknij Ustaw opcje....

5. Pojawi się okno WinHTTrack, kliknij kartę Reguły skanowania i zaznacz pola wyboru dla typów plików, jak pokazano na poniższym zrzucie ekranu; Kliknij OK.

6. Kliknij przycisk Dalej >.

7. Domyślnie przycisk radiowy zostanie wybrany dla opcji W razie potrzeby dostosuj parametry połączenia, a następnie naciśnij przycisk ZAKOŃCZ, aby rozpocząć operację tworzenia kopii lustrzanej. Zaznacz Rozłącz po zakończeniu i kliknij Zakończ, aby rozpocząć tworzenie kopii lustrzanej witryny.

8. Zostanie wyświetlony postęp tworzenia kopii lustrzanej witryny.

9. Po zakończeniu tworzenia kopii lustrzanej witryny WinHTTrack wyświetla komunikat Operacja tworzenia kopii lustrzanej zakończona; kliknij Przeglądaj lustrzaną witrynę internetową.

10. Jeśli pytanie Jak chcesz otworzyć ten plik? pojawi się wyskakujące okienko, wybierz dowolną przeglądarkę internetową i kliknij OK.

11. Uruchamia się lustrzana witryna www.certifiedhacker.com. Adres URL wyświetlany w pasku adresu wskazuje, że obraz witryny jest przechowywany na komputerze lokalnym.

12. Przeanalizuj wszystkie katalogi, HTML, obrazy, pliki flash, wideo i inne pliki dostępne w lustrzanej witrynie docelowej. Możesz także sprawdzić możliwe exploity i luki w zabezpieczeniach. Witryna będzie działać jak witryna hostowana na żywo.

13. Po zakończeniu analizy zamknij okno przeglądarki i kliknij Zakończ w oknie WinHTTrack, aby zakończyć proces.

14. Niektóre witryny są bardzo duże i utworzenie kopii lustrzanej całej witryny może zająć dużo czasu.

15. Atakujący mogą dalej wykorzystywać luki w zabezpieczeniach zidentyfikowane przez HTTrack Website Copier do przeprowadzania różnych ataków aplikacji internetowych na witrynę internetową docelowej organizacji.

16. To kończy demonstrację tworzenia kopii lustrzanej docelowej witryny internetowej za pomocą HTTrack Web Site Copier.

17. Możesz także użyć innych narzędzi do tworzenia kopii lustrzanych, takich jak Cyotek WebCopy (https://www.cyotek.com) itp., aby utworzyć kopię lustrzaną docelowej witryny internetowej.

18. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

19. Wyłącz maszynę wirtualną Windows 11.

Zadanie 6: Zbierz informacje o docelowej witrynie za pomocą GRecon

GRecon to narzędzie Pythona, którego można używać do uruchamiania zapytań w wyszukiwarce Google w celu przeprowadzenia rekonesansu celu w celu znalezienia subdomen, subdomen, stron logowania, list katalogów, ujawnionych dokumentów i wpisów WordPress.

1. Włącz maszynę wirtualną Parrot Security. Na stronie logowania domyślnie zostanie wybrana nazwa użytkownika atakującego. Wprowadź hasło jako toor w polu Hasło i naciśnij Enter, aby zalogować się do urządzenia.

2. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

3. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

4. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

5. Teraz wpisz cd GRecon i naciśnij Enter, aby przejść do katalogu GRecon.

6. W oknie terminala wpisz python3 grecon.py i naciśnij Enter.

7. GRecon inicjalizuje się, w polu Ustaw cel (site.com): wpisz Certifiedhacker.com i naciśnij Enter.

8. GRecon wyszukuje dostępne subdomeny, subdomeny, strony logowania, wykazy katalogów, ujawnione dokumenty, wpisy WordPress i strony do wklejania i wyświetla wyniki.

Uwaga: Wyszukiwanie zajmie około 5 minut.

9. Atakujący mogą dalej wykorzystywać zebrane informacje do przeprowadzania różnych ataków aplikacji internetowych na docelową witrynę.

10. Na tym kończy się demonstracja zbierania informacji o docelowej stronie internetowej za pomocą GRecon.

11. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 7: Zbierz listę słów z witryny docelowej za pomocą CeWL

Słowa dostępne na docelowej stronie internetowej mogą ujawnić krytyczne informacje, które mogą pomóc w dalszym wykorzystaniu. CeWL to aplikacja ruby, która służy do przeszukiwania określonego docelowego adresu URL do określonej głębokości, opcjonalnie podążając za linkami zewnętrznymi, i zwraca listę unikalnych słów, które można wykorzystać do łamania haseł.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Na maszynie wirtualnej Parrot Security kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

2. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

3. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter.

Uwaga: Wpisane hasło nie będzie widoczne.

4. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

5. W oknie terminala wpisz cewl -d 2 -m 5 www.certifiedhacker.com i naciśnij Enter. Uwaga: -d reprezentuje głębokość pająka na stronie internetowej (tutaj 2), a -m reprezentuje minimalną długość słowa (tutaj 5).

6. Zbierana jest unikalna lista słów z docelowej witryny, jak pokazano na zrzucie ekranu.

Uwaga: Minimalna długość słowa to 5, a głębokość pająka docelowej witryny to 2.

7. Alternatywnie, tę unikalną listę słów można zapisać bezpośrednio do pliku tekstowego. Aby to zrobić, wpisz cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com i naciśnij Enter.

Uwaga: -w - Zapisz dane wyjściowe do pliku (tutaj, wordlist.txt)

8. Domyślnie plik z listą słów jest zapisywany w katalogu głównym. Wpisz pluma wordlist.txt i naciśnij Enter, aby wyświetlić wyodrębnioną listę słów.

9. Zostanie otwarty plik zawierający unikalną listę słów wyodrębnioną z docelowej witryny.

10. Wpisz cewl --help i naciśnij Enter w terminalu Parrot, aby wyświetlić listę dostępnych opcji.

11. Ta lista słów może być dalej wykorzystywana do przeprowadzania ataków brute-force na wcześniej pozyskane wiadomości e-mail pracowników docelowej organizacji.

12. To kończy demonstrację zbierania listy słów z docelowej strony internetowej za pomocą CeWL.

13. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

14. Wyłącz maszynę wirtualną Parrot Security.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj śledzenie poczty e-mail

Śledzenie poczty e-mail lub śledzenie wiadomości e-mail obejmuje analizę nagłówka wiadomości e-mail w celu poznania szczegółowych informacji o nadawcy.

Scenariusz laboratoryjny

Jako profesjonalny etyczny haker musisz być w stanie śledzić wiadomości e-mail osób (pracowników) z docelowej organizacji w celu zebrania krytycznych informacji, które mogą pomóc w zbudowaniu skutecznej strategii hakerskiej. Śledzenie poczty e-mail umożliwia zbieranie informacji, takich jak adresy IP, serwery pocztowe, szczegóły systemu operacyjnego, geolokalizacja, informacje o dostawcach usług zaangażowanych w wysyłanie poczty itp. Wykorzystując te informacje, można przeprowadzać socjotechnikę i inne zaawansowane ataki.

Cele laboratorium

* Zbierz informacje o celu, śledząc wiadomości e-mail za pomocą eMailTrackerPro

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 10 minut

Przegląd funkcji Email Footprinting

Śledzenie wiadomości e-mail lub śledzenie to metoda monitorowania lub szpiegowania wiadomości e-mail dostarczanych do zamierzonego odbiorcy. Ten rodzaj śledzenia jest możliwy dzięki zapisom z cyfrowym znacznikiem czasu, które ujawniają czas i datę, kiedy cel otrzyma i otworzy określoną wiadomość e-mail. E-mail footprinting ujawnia takie informacje jak:

* Systemowy adres IP odbiorcy

* Współrzędne GPS i lokalizacja na mapie odbiorcy

* Kiedy wiadomość e-mail została odebrana i przeczytana

* Rodzaj serwera używanego przez odbiorcę

* Informacje o systemie operacyjnym i przeglądarce

* Jeśli wysłano destrukcyjną wiadomość e-mail

* Czas spędzony na czytaniu wiadomości e-mail

* Czy odbiorca odwiedził jakiekolwiek linki przesłane w wiadomości e-mail

* Pliki PDF i inne rodzaje załączników

* Jeśli wiadomości miały wygasać po określonym czasie

Zadania laboratoryjne

Zadanie 1: Zbierz informacje o celu przez śledzenie e-maili za pomocą eMailTrackerPro

Nagłówek wiadomości e-mail jest kluczową częścią każdej wiadomości e-mail i jest uważany za doskonałe źródło informacji dla każdego etycznego hakera przeprowadzającego ataki na cel. Nagłówek wiadomości e-mail zawiera szczegółowe informacje na temat nadawcy, informacje o trasie, schemat adresowania, datę, temat, odbiorcę itp. Ponadto nagłówek wiadomości e-mail pomaga etycznym hakerom prześledzić ścieżkę trasy, którą przebyła wiadomość e-mail przed dostarczeniem jej do odbiorcy. Tutaj zbierzemy informacje, analizując nagłówek wiadomości e-mail za pomocą eMailTrackerPro.

1. Włącz maszynę wirtualną Windows 11. Zaloguj się za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd. Przejdź do https://emailtrackerpro.softonic.pl/?ex=DINS-635.0.

2. Pobierz i zainstaluj plik.

3. Pojawi się okno konfiguracji eMailTrackerPro. Postępuj zgodnie z instrukcjami kreatora (wybierając opcje domyślne), aby zainstalować eMailTrackerPro.

4. Po zakończeniu instalacji, w kreatorze instalacji eMailTrackerPro, usuń zaznaczenie pola wyboru Pokaż plik Readme i kliknij przycisk Zakończ, aby uruchomić eMailTrackerPro.

5. Pojawi się główne okno eMailTrackerPro wraz z wyskakującym okienkiem Wybór edycji; Kliknij OK.

6. Pojawi się główne okno eMailTrackerPro

7. Aby śledzić nagłówki wiadomości e-mail, kliknij ikonę Moje raporty śledzenia w sekcji Widok (tutaj zobaczysz raport wyjściowy śledzonego nagłówka wiadomości e-mail).

8. Kliknij ikonę Śledzenie nagłówków w sekcji Śledzenie nowej wiadomości e-mail, aby rozpocząć śledzenie.

9. Pojawi się wyskakujące okienko; wybierz Śledź e-mail, który otrzymałem. Skopiuj nagłówek wiadomości e-mail z podejrzanej wiadomości e-mail, którą chcesz śledzić, i wklej go w polu Nagłówki wiadomości e-mail: w sekcji Wprowadź szczegóły.

10. Aby znaleźć nagłówki e-maili, otwórz dowolną przeglądarkę internetową i zaloguj się na dowolne konto e-mail; w skrzynce odbiorczej e-mail otwórz wiadomość, której nagłówki chcesz wyświetlić.

Uwaga: W Gmailu znajdź nagłówek e-maila, wykonując następujące czynności:

* Otwórz wiadomość e-mail; kliknij strzałkę ikony kropek (Więcej) obok ikony Odpowiedz w prawym górnym rogu okienka wiadomości.

* Wybierz Pokaż oryginał z listy.

* Okno oryginalnej wiadomości pojawia się w nowej karcie przeglądarki ze wszystkimi szczegółami

* Wiadomości e-mail, w tym nagłówek wiadomości e-mail

Uwaga: w programie Outlook znajdź nagłówek wiadomości e-mail, wykonując następujące czynności:

* Kliknij dwukrotnie wiadomość e-mail, aby otworzyć ją w nowym oknie

* Kliknij ikonę ... (Więcej działań) znajdującą się po prawej stronie okienka wiadomości, aby otworzyć opcje wiadomości

* W opcjach kliknij Wyświetl

* Pojawi się okno przeglądania źródła wiadomości ze wszystkimi szczegółami dotyczącymi wiadomości e-mail, w tym nagłówka wiadomości e-mail

11. Skopiuj cały tekst nagłówka wiadomości e-mail i wklej go w polu Nagłówki wiadomości e-mail: w eMailTrackerPro i kliknij opcję Śledź.

Uwaga: tutaj analizujemy nagłówek wiadomości e-mail z konta Gmail. Możesz jednak również przeanalizować nagłówek wiadomości e-mail z konta Outlook.

12. Otworzy się okno Moje raporty śledzenia.

13. Lokalizacja e-maila będzie śledzona na mapie (GUI mapy świata). Podsumowanie można również wyświetlić, wybierając opcję Podsumowanie wiadomości e-mail po prawej stronie okna. Sekcja tabeli

tuż pod mapą pokazuje cały przeskok na trasie, wraz z adresem IP i podejrzanymi lokalizacjami dla każdego przeskoku.

14. Aby sprawdzić raport, kliknij przycisk Wyświetl raport nad Mapą, aby wyświetlić pełny raport śledzenia.

15. Pełny raport pojawi się w domyślnej przeglądarce.

Uwaga: Jeśli pojawi się wyskakujące okienko z prośbą o wybranie przeglądarki, wybierz Firefox i kliknij OK.

16. Rozwiń każdą sekcję, aby wyświetlić szczegółowe informacje.

17. To kończy demonstrację zbierania informacji poprzez analizę nagłówka wiadomości e-mail za pomocą eMailTrackerPro.

18. Możesz także użyć narzędzi do śledzenia wiadomości e-mail, takich jak Infoga (https://github.com), Mailtrack (https://mailtrack.io) itp., aby śledzić wiadomość e-mail i wyodrębniać informacje o celu, takie jak tożsamość nadawcy, serwer pocztowy , adres IP nadawcy, lokalizacja itp.

19. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

20. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj Whois Footprinting

Wyszukiwanie Whois ujawnia dostępne informacje o nazwie hosta, adresie IP lub domenie.

Scenariusz laboratoryjny

Podczas procesu footprintingu ważne jest zebranie informacji o docelowym adresie IP i domenie uzyskanych podczas poprzednich etapów zbierania informacji. Jako profesjonalny etyczny haker lub tester penetracyjny powinieneś być w stanie wykonać śledzenie Whois na celu; ta metoda dostarcza informacji o domenie docelowej, takich jak właściciel, jej rejestrator, szczegóły rejestracji, serwer nazw, informacje kontaktowe itp. Korzystając z tych informacji, można stworzyć mapę sieci organizacji, przeprowadzić ataki socjotechniczne i uzyskać wewnętrzne szczegóły dotyczące domeny sieć.

Cele laboratorium

Wykonaj wyszukiwanie Whois za pomocą DomainTools

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 5 minut

Przegląd Footprintingu Whois

To laboratorium skupia się na tym, jak przeprowadzić wyszukiwanie Whois i przeanalizować wyniki. Whois to protokół zapytań i odpowiedzi używany do wysyłania zapytań do baz danych, które przechowują zarejestrowanych użytkowników lub cesjonariuszy zasobu internetowego, takiego jak nazwa domeny, blok adresu IP lub system autonomiczny. Ten protokół nasłuchuje żądań na porcie 43 (TCP). Regionalne rejestry internetowe (RIR) utrzymują bazy danych Whois i zawierają dane osobowe właścicieli domen. Dla każdego zasobu baza danych Whois udostępnia rekordy tekstowe z informacjami o samym zasobie oraz odpowiednimi informacjami o cesjonariuszach, rejestrujących i informacjami administracyjnymi (daty utworzenia i wygaśnięcia).

Zadania laboratoryjne

Zadanie 1: Wykonaj wyszukiwanie Whois za pomocą DomainTools

Tutaj zbierzemy informacje o celu, przeprowadzając wyszukiwanie Whois za pomocą DomainTools.

1. Włącz maszynę wirtualną Windows 11. Zaloguj się do maszyny wirtualnej Windows 11 za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd.

2. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy, wpisz http://whois.domaintools.com i naciśnij Enter. Pojawi się witryna Whois Lookup,

3. Teraz w pasku wyszukiwania Wprowadź domenę lub adres IP... wpisz www.certifiedhacker.com i kliknij Szukaj.

4. Ten wynik wyszukiwania ujawnia szczegóły związane z wprowadzonym adresem URL, www.certifiedhacker.com, w tym szczegóły organizacyjne, takie jak dane rejestracyjne, serwery nazw, adres IP, lokalizacja itp.

5. To kończy demonstrację zbierania informacji o organizacji docelowej poprzez wykonanie wyszukiwania Whois przy użyciu DomainTools.

6. Możesz także użyć innych narzędzi wyszukiwania Whois, takich jak SmartWhois (https://www.tamos.com), Batch IP Converter (http://www.sabsoft.com) itp., aby wyodrębnić dodatkowe docelowe informacje Whois.

7. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

8. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj śledzenie DNS

DNS lub Domain Name System, footprinting ujawnia informacje o danych strefy DNS.

Scenariusz laboratoryjny

Jako profesjonalny etyczny haker musisz zebrać informacje DNS domeny docelowej uzyskane podczas poprzednich kroków. Musisz wykonać analizę DNS, aby zebrać informacje o serwerach DNS, rekordach DNS i typach serwerów używanych przez organizację docelową. Dane stref DNS obejmują nazwy domen DNS, nazwy komputerów, adresy IP, serwery poczty domeny, rekordy usług i wiele innych

informacji o sieci docelowej. Korzystając z tych informacji, możesz określić kluczowe hosty połączone w sieci i przeprowadzić ataki socjotechniczne, aby zebrać jeszcze więcej informacji.

Cele laboratorium

* Zbierz informacje DNS za pomocą narzędzia wiersza poleceń nslookup i narzędzia online

* Wykonaj odwrotne wyszukiwanie DNS za pomocą odwrotnego sprawdzania domeny IP i DNSRecon

* Zbierz informacje o subdomenie i rekordach DNS za pomocą SecurityTrails

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Maszyna wirtualna Parrot Security

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 20 minut

Przegląd DNS

DNS uważany za pośrednie źródło wszelkiej komunikacji internetowej. Podstawową funkcją DNS jest tłumaczenie nazwy domeny na adres IP i odwrotnie, aby umożliwić komunikację człowiek-maszyna-sieć-internet. Ponieważ każde urządzenie ma unikalny adres IP, ludziom trudno jest zapamiętać wszystkie adresy IP wymaganej aplikacji. DNS pomaga w konwersji adresu IP na łatwiejszy do zrozumienia format domeny, co zmniejsza obciążenie ludzi.

Zadania laboratoryjne

Zadanie 1: Zbierz informacje DNS za pomocą narzędzia wiersza poleceń nslookup i narzędzia online

nslookup to narzędzie wiersza poleceń służące do administrowania siecią, zwykle używane do wysyłania zapytań do DNS w celu uzyskania mapowania nazwy domeny lub adresu IP albo dowolnego innego określonego rekordu DNS. To narzędzie jest dostępne zarówno jako narzędzie wiersza polecenia, jak i aplikacja internetowa. Tutaj przeprowadzimy gromadzenie informacji DNS o organizacjach docelowych za pomocą narzędzia wiersza poleceń nslookup i aplikacji internetowej NSLOOKUP.

1. Włącz maszyny wirtualne Windows 11 i Parrot Security.

2. Zaloguj się do maszyny wirtualnej Windows 11 za pomocą nazwy użytkownika: Admin i hasła: Pa$$słowo. Uruchom wiersz polecenia, wpisz nslookup i naciśnij Enter. Spowoduje to wyświetlenie domyślnego serwera i jego adresu przypisanego do komputera z systemem Windows 11.

3. W trybie interaktywnym nslookup wpisz set type=a i naciśnij Enter. Ustawienie typu jako „a” konfiguruje nslookup do zapytania o adres IP danej domeny.

4. Wpisz domenę docelową www.certifiedhacker.com i naciśnij Enter. Spowoduje to rozpoznanie adresu IP i wyświetlenie wyniku

5. Pierwsze dwie linie wyniku to:

Serwer: dns.google i adres: 8.8.8.8

Oznacza to, że wynik został skierowany do domyślnego serwera hostowanego na komputerze lokalnym (Windows 11), który rozpoznaje żądaną domenę.

6. Tak więc, jeśli odpowiedź pochodzi z serwera komputera lokalnego (Google), ale nie z serwera, który zgodnie z prawem hostuje domenę www.certifiedhacker.com; jest uważana za nieautorytatywną odpowiedź. Tutaj adres IP domeny docelowej www.certifiedhacker.com to 162.241.216.11.

7. Ponieważ zwrócony wynik nie jest autorytatywny, musisz uzyskać autorytatywny serwer nazw domeny.

8. Wpisz set type=cname i naciśnij Enter. Wyszukiwanie CNAME odbywa się bezpośrednio na autorytatywnym serwerze nazw domeny i wyświetla rekordy CNAME dla domeny.

9. Wpisz Certifiedhacker.com i naciśnij Enter.

10. Spowoduje to zwrócenie autorytatywnego serwera nazw domeny (nsl.bluehost.com) wraz z adresem serwera poczty (dnsadmin.box5331.bluehost.com).

11. Ponieważ uzyskałeś autorytatywny serwer nazw, będziesz musiał określić adres IP serwera nazw.

12. Wydaj komendę set type=a i naciśnij Enter.

13. Wpisz nsl.bluehost.com (lub główny serwer nazw wyświetlany w środowisku laboratoryjnym) i naciśnij klawisz Enter. Spowoduje to zwrócenie adresu IP serwera.

14. Autorytatywny serwer nazw przechowuje rekordy związane z domeną. Tak więc, jeśli osoba atakująca może określić autorytatywny serwer nazw (podstawowy serwer nazw) i uzyskać powiązany z nim adres IP, może próbować wykorzystać ten serwer do przeprowadzania ataków, takich jak DoS, DDoS, przekierowanie adresu URL itp.

15. Możesz także wykonać te same operacje za pomocą narzędzia online NSLOOKUP. Przeprowadź serię zapytań i przejrzyj informacje, aby zapoznać się z narzędziem NSLOOKUP i zebrać informacje.

16. Teraz użyjemy narzędzia online NSLOOKUP do zebrania informacji DNS o domenie docelowej.

17. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy i wpisz http://www.kloth.net/services/nslookup.php i naciśnij Enter.

18. Zostanie wyświetlona strona internetowa NSLOOKUP.

19. Po otwarciu witryny, w polu Domena: wpisz Certifiedhacker.com. Ustaw pole Zapytanie: na wartość domyślną [A (adres IPv4)] i kliknij przycisk Wyszukaj, aby przejrzeć wyświetlone wyniki.

20. W polu Zapytanie: kliknij strzałkę listy rozwijanej i zaznacz różne dostępne opcje.

21. Jak widać jest opcja na AAAA (adres IPv6); wybierz to i kliknij Wyszukaj. Wykonaj zapytania z tym związane, ponieważ istnieją ataki, które są możliwe również w sieciach IPv6.

22. To kończy demonstrację zbierania informacji DNS za pomocą narzędzia wiersza poleceń nslookup i narzędzia online NSLOOKUP. 23. Możesz także użyć narzędzi do wyszukiwania DNS, takich jak DNSdumpster (https://dnsdumpster.com), DNS Records (https://network-tools.com) itp., aby wyodrębnić dodatkowe informacje o docelowym DNS.

24. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Wykonaj wsteczne wyszukiwanie DNS za pomocą wstecznego sprawdzania domeny IP i DNSRecon

Wyszukiwanie DNS służy do wyszukiwania adresów IP dla danej nazwy domeny, a operacja odwrotnego DNS jest wykonywana w celu uzyskania nazwy domeny o podanym adresie IP. Tutaj przeprowadzimy odwrotne wyszukiwanie DNS za pomocą narzędzia do sprawdzania domeny Reverse IP Domain Check, aby znaleźć inne domeny/witryny, które współdzielą ten sam serwer WWW, co nasz serwer docelowy. W tym przypadku przeprowadzimy również odwrotne wyszukiwanie DNS za pomocą DNSRecon w zakresie adresów IP, próbując zlokalizować rekord DNS PTR dla tych adresów IP.

1. Na maszynie wirtualnej Windows 11 otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.yougetsignal.com i naciśnij Enter.

2. Pojawi się sygnał strony internetowej, kliknij Odwróć sprawdzanie domeny IP.

3. Na stronie Reverse IP Domain Check wpisz www.certifiedhacker.com w polu Adres zdalny i kliknij Sprawdź, aby znaleźć inne domeny/witryny hostowane na serwerze sieciowym Certifiedhacker.com. Otrzymasz listę domen/stron hostowanych na tym samym serwerze co www.certifiedhacker.com,

4. Teraz przełącz się na maszynę wirtualną Parrot Security.

5. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

6. W oknie Parrot Terminal wpisz cd dnsrecon i naciśnij Enter, aby wejść do katalogu dnsrecon.

7. Wpisz chmod +x ./dnsrecon.py i naciśnij Enter.

8. Teraz wpisz ./dnsrecon.py -r 162.241.216.0-162.241.216.255 i naciśnij klawisz Enter, aby zlokalizować rekord DNS PTR dla adresów IP z zakresu od 162.241.216.0 do 162.241.216.255.

Uwaga: Tutaj użyjemy zakresu adresów IP, który obejmuje adres IP naszego celu, czyli domeny Certifiedhacker.com (162.241.216.11), którą uzyskaliśmy w poprzednich krokach.

Uwaga: Opcja -r określa zakres adresów IP (od pierwszego do ostatniego) dla brutalnej siły wyszukiwania wstecznego.

9. Na tym kończy się demonstracja zbierania informacji o organizacji docelowej poprzez wykonanie odwrotnego wyszukiwania DNS przy użyciu narzędzia Reverse IP Domain Check i DNSRecon „otrzymasz sygnał”.

10. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

11. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 3: Zbierz informacje o subdomenie i rekordach DNS za pomocą SecurityTrails

SecurityTrails to zaawansowane narzędzie do wyliczania DNS, które jest w stanie stworzyć mapę DNS docelowej sieci domeny. Może wyliczać zarówno bieżące, jak i historyczne rekordy DNS, takie jak A, AAAA, NS, MX, SOA i TXT, co pomaga w budowaniu struktury DNS, a także wylicza wszystkie istniejące subdomeny domeny docelowej za pomocą technik brute-force. W tym przypadku użyjemy SecurityTrails do zebrania informacji dotyczących subdomen i rekordów DNS docelowej witryny.

1. Przełącz się na maszynę wirtualną Windows 11.

2. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy i wpisz https://securitytrails.com/ i naciśnij Enter.

3. Pojawi się strona SecurityTrails. W witrynie kliknij przycisk Zarejestruj się za darmo w prawym górnym rogu strony.

4. Zostanie wyświetlona strona Zarejestruj się — za darmo, wprowadź wymagane dane i zaznacz pole wyboru warunków. Kliknij Zarejestruj się za darmo.

5. Na podany adres e-mail zostanie wysłana wiadomość weryfikacyjna.

6. Otwórz nową kartę w przeglądarce i zaloguj się na konto e-mail podane podczas rejestracji. Otwórz wiadomość otrzymaną od Security! - szyny i kliknij Potwierdź adres e-mail.

7. Po pomyślnej weryfikacji zostaniesz przekierowany do Dashboard na stronie SecurityTrails.

8. W polu Wprowadź domenę, adres IP, słowo kluczowe lub nazwę hosta wpisz Certifiedhacker.com i naciśnij Enter.

9. Pojawią się rekordy DNS Certifiedhacker.com, zawierające rekordy A, rekordy AAAA, rekordy MX, rekordy NS, rekordy SOA, rekordy TXT i rekordy CNAME

10. Po przejrzeniu zakładki rekordów DNS przejdź do zakładki Dane historyczne, gdzie znajdziesz dane historyczne rekordów A, AAAA, MX, NS, SOA i TXT.

11. Teraz przejdź do zakładki Subdomeny, gdzie znajdziesz wszystkie powiązane subdomeny certyfiiedhaker.com.

12. Rekordy DNS dostarczają ważnych informacji o lokalizacjach i typach serwerów, których atakujący mogą użyć do dalszych ataków na aplikacje internetowe.

13. Na tym kończy się demonstracja zbierania informacji o subdomenie i rekordach DNS organizacji docelowej za pomocą SecurityTrails.

14. Możesz także użyć DNSChecker (https://dnschecker.org) i DNSdumpster (https://dnsdumpster.com) itp., aby wykonać śledzenie DNS na docelowej stronie internetowej.

15. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

16. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Wykonaj badanie śladu sieciowego

Śledzenie sieci to proces zbierania informacji związanych z siecią organizacji docelowej.

Scenariusz laboratoryjny

Dysponując adresem IP, nazwą hosta i domeną uzyskanymi w poprzednich krokach zbierania informacji, kolejnym zadaniem profesjonalnego etycznego hakera jest wykonanie pomiarów sieci w celu zebrania informacji związanych z siecią organizacji docelowej, takich jak zasięg sieci, trasa śledzenia, TTL wartości itp. Te informacje pomogą ci stworzyć mapę docelowej sieci i przeprowadzić atak typu man-in-the-middle.

Cele laboratorium

* Znajdź zasięg sieci

* Wykonaj śledzenie sieci na komputerach z systemem Windows i Linux

* Wykonuj zaawansowane śledzenie tras sieciowych za pomocą Path Analyzer Pro

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Maszyna wirtualna Parrot Security

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 15 minut

Omówienie śladu sieciowego

Footprinting sieci to proces gromadzenia danych dotyczących określonego środowiska sieciowego. Umożliwia etycznym hakerom narysowanie schematu sieci i bardziej szczegółową analizę sieci docelowej w celu przeprowadzenia zaawansowanych ataków.

Zadania laboratoryjne

Zadanie 1: Znajdź zasięg sieci

Informacje o zasięgu sieci pomagają w tworzeniu mapy sieci docelowej. Korzystając z zasięgu sieci, możesz zbierać informacje o tym, jak jest zbudowana sieć i które maszyny w sieciach działają. Ponadto pomaga również zidentyfikować topologię sieci i uzyskać dostęp do urządzenia sterującego i systemu operacyjnego używanego w sieci docelowej. Tutaj zlokalizujemy zasięg sieci za pomocą narzędzia do wyszukiwania bazy danych ARIN Whois.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Włącz maszynę wirtualną z systemem Windows 11. Zaloguj się za pomocą nazwy użytkownika: Admin i hasła: Pa$$wOrd.

2. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy i wpisz https://www.arin.net/about/welcome/region i naciśnij Enter.

Uwaga: Jeśli w górnej części przeglądarki pojawi się powiadomienie o bardziej bezpiecznych, szyfrowanych wyszukiwaniach DNS, kliknij opcję Wyłącz.

3. Pojawi się witryna ARIN, w pasku wyszukiwania wprowadź adres IP docelowej organizacji (tutaj docelowa organizacja to Certifiedhacker.com, której adres IP to 162.241.216.11), a następnie kliknij przycisk Szukaj.

4. Otrzymasz informacje o zasięgu sieci wraz z innymi informacjami, takimi jak typ sieci, dane rejestracyjne itp.

5. To kończy demonstrację lokalizowania zasięgu sieci za pomocą narzędzia wyszukiwania bazy danych ARIN Whois.

6. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Wykonaj śledzenie sieci na komputerach z systemem Windows i Linux

Trasa to ścieżka, którą pokonuje pakiet sieciowy między źródłem a miejscem docelowym. Śledzenie sieci to proces identyfikowania ścieżki i hostów leżących między źródłem a miejscem docelowym. Śledzenie sieci dostarcza krytycznych informacji, takich jak adresy IP hostów leżących między źródłem a miejscem docelowym, co umożliwia mapowanie topologii sieci w organizacji. Traceroute może służyć do wydobywania informacji o topologii sieci, zaufanych routerach, lokalizacjach zapór ogniowych itp. Tutaj wykonamy śledzenie sieci na komputerach z systemem Windows i Linux.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Na maszynie wirtualnej z systemem Windows 11 otwórz okno wiersza polecenia. Wpisz tracert www.certifiedhacker.com i naciśnij Enter, aby wyświetlić przeskoki, które pakiety wykonały przed dotarciem do miejsca docelowego.

2. Wpisz tracert /? i naciśnij klawisz Enter, aby wyświetlić różne opcje polecenia

3. Wpisz tracert -h 5 www.certifiedhacker.com i naciśnij Enter, aby wykonać śledzenie, ale z maksymalnie 5 dozwolonymi przeskokami.

4. Po wyświetleniu wyniku zamknij okno wiersza polecenia.

5. Włącz maszynę wirtualną Parrot Security. Na stronie logowania domyślnie zostanie wybrana nazwa użytkownika atakującego. Wprowadź hasło jako toor w polu Hasło i naciśnij Enter, aby zalogować się do urządzenia.

Notatka:

* Jeśli wyskakujące okienko Parrot Updater pojawi się w prawym górnym rogu pulpitu, zignoruj je i zamknij.

* Jeśli pojawi się wyskakujące okienko Pytania z prośbą o aktualizację urządzenia, kliknij Nie, aby zamknąć okno.

6. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

7. Pojawi się okno Parrot Terminal. W oknie terminala wpisz traceroute www.certifiedhacker.com i naciśnij Enter, aby zobaczyć przeskoki, które pakiety wykonały przed dotarciem do miejsca docelowego.

Uwaga: Ponieważ stworzyliśmy prostą sieć, możesz znaleźć bezpośredni przeskok ze źródła do miejsca docelowego. Jednak zrzuty ekranu mogą się różnić w zależności od miejsca docelowego.

8. Na tym kończy się demonstracja wykonywania trasowania sieciowego przy użyciu komputerów z systemami Windows i Linux.

9. Możesz także użyć innych narzędzi traceroute, takich jak VisualRoute (http://www.visualroute.com), Traceroute NG (https://www.solarwinds.com) itp., aby wyodrębnić dodatkowe informacje o sieci docelowej organizacji.

10. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

11. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 3: Wykonaj zaawansowane śledzenie tras sieciowych za pomocą Path Analyzer Pro

Path Analyzer Pro wykonuje śledzenie tras sieciowych za pomocą testów wydajności, DNS, Whois i rozdzielczości sieci w celu zbadania problemów z siecią. Tutaj wykonamy śledzenie sieci za pomocą Path Analyzer Pro.

1. Na maszynie wirtualnej Windows 11 otwórz Eksplorator plików i przejdź do https://path-analyzer-pro.software.informer.com/2.7/.

2. Pobierz i zainstaluj plik.

3. Postępuj zgodnie z instrukcjami kreatora (wybierając opcje domyślne), aby zainstalować Path Analyzer Pro.

Uwaga: Jeśli pojawi się okno Kontrola konta użytkownika, kliknij Tak.

4. Kliknij Szukaj na pulpicie. Wpisz path analyzer w polu wyszukiwania, Path Analyzer Pro 2.7 pojawi się w wynikach, kliknij Uruchom jako administrator, aby go uruchomić.

Uwaga: Jeśli pojawi się okno Kontrola konta użytkownika, kliknij Tak.

5. Pojawi się okno Path Analyzer Pro wraz z wyskakującym okienkiem Formularz rejestracyjny; Kliknij Oceń w wyskakującym okienku.

6. W lewym panelu okna Path Analyzer Pro kilka opcji jest ustawionych jako domyślne w sekcjach Opcje standardowe i Szczegóły zaawansowanej sondy. Upewnij się, że przycisk radiowy ICMP w polu Protokół w Opcjach standardowych jest wybrany, a opcja Inteligentna w polu Długość pakietu w sekcji Szczegóły zaawansowanej sondy jest zaznaczona.

Uwaga: Jeśli masz zaporę ogniową, należy ją wyłączyć, aby uzyskać odpowiednie wyniki.

7. W sekcji Zaawansowane szczegóły śledzenia kilka opcji jest ustawionych jako domyślne. Upewnij się, że opcja Zatrzymaj przy komunikatach kontrolnych (ICMP) jest zaznaczona w sekcji Szczegóły zaawansowanego śledzenia.

8. Aby wykonać śledzenie, wprowadź nazwę hosta w polu Cel (na przykład www.google.com) i upewnij się, że opcja Smart w polu Port jest zaznaczona (tutaj domyślnie jest to 65535). Z menu rozwijanego wybierz Śledzenie czasowe i kliknij Śledź.

9. Pojawi się okno dialogowe Typ czasu śledzenia. Określ czas śledzenia (tutaj mm zmienia się na 3) w formacie hh:mm:ss i kliknij Akceptuj.

10. Gdy Path Analyzer Pro wykonuje ten ślad, przycisk Śledź zmienia się automatycznie na Stop.

Uwaga: Jeśli pojawi się wyskakujące okienko odczytu, kliknij OK.

11. Po zakończeniu śledzenia wyniki śledzenia są wyświetlane w zakładce Raport w postaci wykresu liniowego przedstawiającego liczbę przeskoków między użytkownikiem a celem.

12. Kliknij kartę Synopsis, która wyświetla jednostronicowe podsumowanie wyników śledzenia.

13. Kliknij kartę Wykresy, aby wyświetlić wyniki śledzenia.

14. Kliknij Geo, co spowoduje wyświetlenie mapy świata trasy śledzenia.

15. Kliknij kartę Dziennik, aby wyświetlić bieżący dziennik śledzenia i dziennik sesji.

16. Kliknij kartę Statystyki, która zawiera statystyki życia bieżącego śladu.

17. Kliknij Eksportuj na pasku narzędzi, aby wyeksportować raport.

18. Pojawi się okno Zapisz statystyki jako. Podaj żądaną nazwę pliku w polu Nazwa pliku: (tutaj, Przykładowy raport) i kliknij Zapisz.

Uwaga: Domyślnie raport zostanie zapisany w C:\Program Files (x86)\Path Analyzer Pro 2.7. Możesz jednak zmienić go na preferowaną lokalizację.

19. Na tym kończy się demonstracja zbierania informacji o docelowej organizacji przez wykonywanie śledzenia sieci za pomocą Path Analyzer Pro.

20. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

21. Wyłącz maszynę wirtualną Windows 11.

Analiza laboratoryjna

Przeanalizuj i udokumentuj wyniki tego ćwiczenia laboratoryjnego.

Przeprowadzaj Footprinting za pomocą różnych narzędzi Footprinting Etyczni hakerzy i testerzy penetracji wykonują footprinting za pomocą różnych narzędzi, które sprawiają, że zbieranie informacji jest łatwym zadaniem.

Scenariusz laboratoryjny

Informacje zebrane w poprzednich krokach mogą nie wystarczyć do ujawnienia potencjalnych słabych punktów celu. Dostępnych może być więcej informacji, które mogłyby pomóc w znalezieniu luk w celu. Jako etyczny haker powinieneś szukać jak najwięcej informacji o celu za pomocą różnych narzędzi. To ćwiczenie laboratoryjne zademonstruje, jakie inne informacje można wyodrębnić z celu za pomocą różnych narzędzi do śledzenia śladów.

Cele laboratorium

* Footprinting za pomocą Recon-ng

* Footprinting za pomocą Maltego

* Footprinting przy użyciu OSRFramework

* Footprinting przy użyciu FOCA

* Footprinting za pomocą BillCipher

* Footprinting celu przy użyciu OSINT Framework

Środowisko laboratoryjne

Do wykonania tego laboratorium potrzebujesz:

* Maszyna wirtualna Windows 11

* Maszyna wirtualna Parrot Security

* Maszyna wirtualna Windows Server 2019

* Przeglądarki internetowe z połączeniem internetowym

* Uprawnienia administratora do uruchamiania narzędzi

Czas trwania laboratorium

Czas: 65 minut

Przegląd narzędzi Footprinting

Narzędzia Footprinting służą do zbierania podstawowych informacji o systemach docelowych w celu ich wykorzystania. Informacje zebrane przez narzędzia do śledzenia zawierają informacje o lokalizacji adresu IP celu, informacje o routingu, informacje biznesowe, adres, numer telefonu i numer ubezpieczenia społecznego, szczegóły dotyczące źródła wiadomości e-mail i pliku, informacje DNS, informacje o domenie itp.

Zadania laboratoryjne

Zadanie 1: Ślad celu za pomocą Recon-ng

Recon-ng to platforma do rekonesansu internetowego z niezależnymi modułami i interakcją z bazą danych, która zapewnia środowisko, w którym można przeprowadzić rekonesans oparty na sieci Web typu open source. Flere, użyjemy Recon-ng do przeprowadzenia rekonesansu sieci, zebranie informacje o personelu i gromadzenie informacji o celu z portali społecznościowych.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

Uwaga: Uzyskane wyniki mogą się różnić podczas wykonywania tego zadania laboratoryjnego.

1. Włącz maszynę wirtualną Parrot Security. Na stronie logowania domyślnie zostanie wybrana nazwa użytkownika atakującego. Wprowadź hasło jako toor w polu Hasło i naciśnij Enter, aby zalogować się do urządzenia.

Notatka:

* Jeśli wyskakujące okienko Parrot Updater pojawi się w prawym górnym rogu pulpitu, zignoruj je i zamknij.

* Jeśli pojawi się wyskakujące okienko Pytania z prośbą o aktualizację urządzenia, kliknij Nie, aby zamknąć okno.

2. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

3. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

4. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

5. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

6. W oknie Terminal wpisz polecenie recon-ng i naciśnij Enter, aby uruchomić aplikację.

7. Wpisz help i naciśnij Enter, aby wyświetlić wszystkie polecenia, które umożliwiają dodawanie/usuwanie rekordów do bazy danych, wysyłanie zapytań do bazy danych itp.

8. Wpisz marketplace install all i naciśnij Enter, aby zainstalować wszystkie moduły dostępne w recon-ng.

Uwaga: Zignoruj błędy podczas uruchamiania polecenia.

9. Po zainstalowaniu modułów wpisz polecenie wyszukiwania modułów i naciśnij Enter.

Spowoduje to wyświetlenie wszystkich modułów dostępnych w recon-ng.

10. Będziesz mógł przeprowadzić wykrywanie sieci, eksploatację, rekonesans itp., ładując wymagane moduły.

11. Wpisz komendę workspaces i naciśnij Enter. Spowoduje to wyświetlenie poleceń związanych z obszarami roboczymi.

12. Utwórz obszar roboczy do przeprowadzenia rekonesansu sieci. W tym zadaniu utworzymy obszar roboczy o nazwie CEH.

13. Aby utworzyć obszar roboczy, wpisz polecenie workspaces create CEH i naciśnij klawisz Enter. Spowoduje to utworzenie obszaru roboczego o nazwie CEH.

Uwaga: Alternatywnie można wydać polecenie workspaces select CEH, aby utworzyć obszar roboczy o nazwie CEH. Zignoruj błędy podczas uruchamiania poleceń

14. Wejdź na listę obszarów roboczych. Spowoduje to wyświetlenie listy obszarów roboczych (wraz z obszarem roboczym dodanym w poprzednim kroku), które są obecne w bazach danych obszarów roboczych.

15. Dodaj domenę, w której chcesz przeprowadzić rekonesans sieci.

16. Wpisz polecenie db insert domains i naciśnij Enter.

17. W opcji domeny (TEKST) wpisz Certifiedhacker.com i naciśnij Enter. W opcji notatki (TEKST) naciśnij Enter. Spowoduje to dodanie Certifiedhacker.com do obecnego obszaru roboczego.

18. Możesz wyświetlić dodaną domenę, wydając polecenie show domains, jak pokazano na zrzucie ekranu.

19. Zbierz informacje dotyczące hostów powiązane z certyfikowaną witryną hacker.com, ładując moduły rozpoznania sieci, takie jak brute_hosts, Netcraft i Bing.

20. Wpisz moduły ładowania brutalnego i naciśnij klawisz Enter, aby wyświetlić wszystkie moduły związane z brutalnym wymuszaniem. W tym zadaniu będziemy używać modułu recon/domains-hosts/brute_hosts do zbierania hostów.

21. Aby załadować moduł recon/domains-hosts/brute_hosts, wpisz polecenie module load recon/domains-hosts/brute_hosts i naciśnij Enter.

22. Wpisz uruchom i naciśnij Enter. To zaczyna zbierać gospodarzy

23. Zauważ, że hosty zostały dodane, uruchamiając recon/domains-hosts/brute_hosts moduł.

24. Zebrałeś teraz hosty powiązane z Certifiedhacker.com za pomocą modułu brute_hosts. Możesz użyć innych modułów, takich jak Netcraft i Bing, aby zebrać więcej hostów.

Uwaga: Użyj polecenia back, aby wrócić do terminala atrybutów CEH.

Uwaga: Aby rozpoznać hosty za pomocą modułu Bing, użyj następujących poleceń:

* back

* modules load recon/domains-hosts/bing_domain_web

* run

25. Teraz wykonaj wyszukiwanie wsteczne dla każdego adresu IP (adresu IP uzyskanego podczas procesu rekonesansu), aby znaleźć odpowiednie nazwy hostów.

26. Wpisz polecenie module load reverse_resolve i naciśnij klawisz Enter, aby wyświetlić wszystkie moduły powiązane ze słowem kluczowym reverse_resolve. W tym zadaniu będziemy używać modułu recon/hosts-hosts/reverse_resolve.

27. Wpisz polecenie module load recon/hosts-hosts/reverse_resolve i naciśnij klawisz Enter, aby załadować moduł.

28. Wydaj komendę run, aby rozpocząć wyszukiwanie wsteczne.

29. Po zakończeniu procesu wyszukiwania wstecznego wpisz polecenie show hosts i naciśnij klawisz Enter. Spowoduje to wyświetlenie wszystkich żywicieli, które zostały zebrane do tej pory, jak pokazano na zrzucie ekranu.

30. Teraz wpisz polecenie back i naciśnij Enter, aby wrócić do terminala atrybutów CEH.

31. Teraz, gdy zebrałeś kilka hostii, przygotujemy raport zawierający wszystkie hostie.

32. Wpisz polecenie raportowania ładowania modułów i naciśnij klawisz Enter, aby wyświetlić wszystkie moduły powiązane ze słowem kluczowym raportowania. W tym laboratorium zapiszemy raport w formacie HTML. Tak więc używanym modułem jest raportowanie/html.

33. Wpisz polecenie moduły ładuj raportowanie/html i naciśnij klawisz Enter.

34. Zwróć uwagę, że musisz przypisać wartości dla opcji CREATOR i CUSTOMER, gdy wartość NAZWA PLIKU jest już ustawiona i możesz zmienić tę wartość, jeśli to konieczne.

35. Wpisz:

* options set FILENAME /home/attacker/Desktop/results.html i naciśnij Enter. Wydając to polecenie, ustawiasz nazwę raportu jako Results.html i ścieżkę do przechowywania pliku jako Pulpit.

* options set CREATOR [your name] (tutaj Jason) i naciśnij Enter.

* options set CUSTOMER Certifiedhacker Networks (ponieważ masz wykonawcę rekonesansu sieciowego w domenie Certifiedhacker.com) i naciśnij Enter.

36. Wpisz polecenie uruchomienia i naciśnij klawisz Enter, aby utworzyć raport dla wszystkich hostów, które zostały zebrane.

37. Wygenerowany raport jest zapisywany w /home/attacker/Desktop/.

38. Kliknij Miejsca w górnej części Pulpitu i kliknij Folder domowy z rozwijanych opcji.

39. Pojawia się okno atakującego.

40. W oknie atakującego kliknij dwukrotnie Pulpit.

41. Pojawi się okno pulpitu, kliknij prawym przyciskiem myszy plik Results.html, kliknij Otwórz za pomocą i wybierz przeglądarkę Firefox z dostępnych opcji.

42. Wygenerowany raport pojawia się w przeglądarce Firefox, wyświetlając podsumowanie zebranych hostów.

43. Możesz rozwinąć węzeł Hosty, aby wyświetlić wszystkie zebrane hosty.

44. Zamknij wszystkie otwarte okna.

45. Do tej pory używaliśmy narzędzia Recon-ng do przeprowadzania rekonesansu sieci w domenie docelowej

46. Teraz użyjemy Recon-ng do zebrania informacji o personelu.

47. Otwórz nowe okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

48. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

49. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

50. Wpisz recon-ng i naciśnij Enter.

51. Dodaj obszar roboczy, wydając polecenie workspaces create reconnaissance i naciśnij Enter. Spowoduje to utworzenie obszaru roboczego o nazwie reconnaissance.

52. Ustaw domenę i wykonaj na niej footprint, aby wyodrębnić kontakty dostępne w domenie.

53. Wpisz module load recon/domains-contacts/whois_pocs i naciśnij Enter. Ten moduł wykorzystuje ARIN Whois RWS do zbierania danych POC z zapytań Whois dla danej domeny.

54. Wpisz polecenie info i naciśnij klawisz Enter, aby wyświetlić opcje wymagane do uruchomienia tego modułu.

55. Wpisz options set SOURCE facebook.com i naciśnij Enter, aby dodać facebook.com jako domenę docelową.

Uwaga: tutaj używamy facebook.com jako domeny docelowej do zbierania danych kontaktowych.

56. Wpisz polecenie uruchomienia i naciśnij klawisz Enter. Moduł recon/domains-contacts/whois_pocs wyodrębnia kontakty powiązane z domeną i wyświetla je, jak pokazano na zrzucie ekranu

57. Wpisz wstecz i naciśnij Enter, aby wrócić do terminala obszarów roboczych (rozpoznawczych).

58. Do tej pory pozyskaliśmy kontakty związane z domenami. Zanotuj nazwy tych kontaktów.

59. Teraz zweryfikujemy istnienie nazw (nazw użytkownika) na określonych stronach internetowych.

60. Moduł recon/profiles-profiles/namechk weryfikuje istnienie nazwy użytkownika określonego kontaktu. Kontakt, którego użyjemy w tym laboratorium, to Mark Zuckerberg.

61. Wpisz polecenie module load recon/profiles-profiles/namechk i naciśnij klawisz Enter, aby załadować ten moduł.

62. Wpisz zestaw opcji SOURCE MarkZuckerberg i naciśnij Enter. To polecenie ustawia Marka Zuckerberga jako źródło, dla którego chcesz znaleźć istnienie użytkownika na określonych stronach internetowych.

63. Wpisz uruchom i naciśnij Enter. To rozpoczyna wyszukiwanie słowa kluczowego MarkZuckerberg na różnych stronach internetowych.

64. Recon-ng rozpoczyna wyszukiwanie w Internecie obecności nazwy użytkownika na stronach internetowych iw przypadku znalezienia zwraca wynik o treści „User Exists!". Tutaj nie uzyskuje się żadnych wyników.

65. Wpisz polecenie back i naciśnij klawisz Enter, aby wrócić do terminala obszarów roboczych (rozpoznawczych).

66. Aby znaleźć profile użytkowników na różnych stronach internetowych, musisz załadować moduł recon/profiles-profiles/profiler.

67. Wpisz polecenie module load recon/profiles-profiles/profiler i naciśnij klawisz Enter.

68. Wpisz polecenie zestawu opcji SOURCE MarkZuckerberg i naciśnij klawisz Enter.

69. Wpisz polecenie uruchomienia i naciśnij klawisz Enter. Moduł recon/profiles-profiles/profiler wyszukuje tę nazwę użytkownika i zwraca adres URL profilu (znaleziony z pasującą nazwą użytkownika):

Uwaga: Zignoruj wszelkie błędy otrzymane w wynikach.

Uwaga: Podczas wykonywania tego zadania wyniki mogą się różnić.

70. Wpisz wstecz i naciśnij Enter, aby wrócić do terminala obszarów roboczych.

71. Po zweryfikowaniu istnienia użytkownika i uzyskaniu adresu URL profilu przygotujemy raport zawierający wynik.

72. Wpisz polecenie moduły ładuj raportowanie/html i naciśnij klawisz Enter. Przypisz wartości NAZWA PLIKU, Twórca i KLIENT.

Uwaga: W tym zadaniu zapisujemy raport w formacie HTML; dlatego używany jest moduł raportowania/html.

73. Wpisz:

* options set FILENAME /home/attacker/Desktop/Reconnaissance.html i naciśnij Enter. Wydając to polecenie, ustawiasz nazwę raportu jako Reconnaissance.html i ścieżkę do przechowywania pliku jako Pulpit.

* options set CREATOR [your name] (tutaj Jason) i naciśnij Enter.

* options set CUSTOMER Mark Zuckerberg (ponieważ zebrałeś informacje na temat Marka Zuckerberga) i naciśnij Enter.

74. Po wprowadzeniu powyższych informacji wpisz polecenie run i naciśnij Enter, aby utworzyć raport dla wszystkich zebranych żywicieli, jak pokazano na zrzucie ekranu.

75. Wygenerowany raport jest zapisywany w /home/attacker/Desktop/.

76. Kliknij Miejsca w górnej części Pulpitu i kliknij Folder domowy z rozwijanych opcji.

77. Pojawia się okno atakującego.

78. W oknie atakującego kliknij dwukrotnie Pulpit.

79. Pojawi się okno pulpitu, kliknij prawym przyciskiem myszy plik Reconnaissance.html, kliknij Otwórz za pomocą i wybierz przeglądarkę Firefox z dostępnych opcji.

80. Wygenerowany raport pojawia się w przeglądarce Firefox, wyświetlając podsumowanie wyniku. Możesz rozwinąć węzły Kontakty i Profile, aby wyświetlić wszystkie uzyskane wyniki.

81. Możesz dodatkowo rozwinąć węzeł Kontakty i Profile, aby wyświetlić szczegółowe informacje o celu.

Uwaga: Aby wyświetlić szczegółowe informacje o profilach w raporcie, przewiń w prawo.

82. Zebraliśmy teraz informacje o pracowniku pracującym w docelowej organizacji. Zamknij wszystkie otwarte okna.

83. Teraz użyjemy narzędzia Recon-ng do wyodrębnienia listy subdomen i adresów IP powiązanych z docelowym adresem URL.

84. Otwórz nowe okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

85. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

86. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

87. Wpisz recon-ng i naciśnij Enter.

88. Aby wyodrębnić listę subdomen i adresów IP powiązanych z docelowym adresem URL, we

trzeba załadować moduł recon/domains-hosts/hackertarget.

89. Wpisz polecenie module load recon/domains-hosts/hackertarget i naciśnij Enter.

90. Wpisz polecenie zestawu opcji SOURCE Certifiedhacker.com i naciśnij klawisz Enter.

91. Wpisz polecenie uruchomienia i naciśnij klawisz Enter. Recon/domeny-hosty/hackertarget moduł wyszukuje listę subdomen i adresów IP powiązanych z docelowym adresem URL i zwraca listę subdomen i ich adresów IP.

92. To kończy demonstrację zbierania informacji o gospodarzu domeny docelowej i zbierania informacji personelu docelowej organizacji.

93. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 2: Wyznaczanie śladu celu za pomocą Maltego

Maltego to narzędzie do śledzenia śladów używane do zbierania maksymalnej ilości informacji w celu etycznego hakowania, informatyki śledczej i pentestów. Zapewnia bibliotekę transformacji do wyszukiwania danych z otwartych źródeł i wizualizuje te informacje w formacie wykresu, odpowiednim do analizy powiązań i eksploracji danych. Maltego zapewnia interfejs graficzny, który sprawia, że oglądanie tych relacji jest natychmiastowe i dokładne, a nawet umożliwia dostrzeżenie ukrytych połączeń. Tutaj zbierzemy różne informacje o docelowej organizacji za pomocą Maltego.

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. W maszynie wirtualnej Parrot Security otwórz terminal i wpisz sudo maltego i naciśnij Enter, aby uruchomić Maltego.

2. W graficznym interfejsie użytkownika Maltego pojawia się kreator wyboru produktu; kliknij opcję Uruchom z Maltego CE (bezpłatny).

Uwaga: Jeśli pojawi się wyskakujące okienko Zoptymalizowane ustawienia pamięci, kliknij Uruchom ponownie teraz.

3. Gdy pojawi się okno Konfiguruj Maltego wraz z formularzem UMOWA LICENCYJNA, zaznacz pole Akceptuj i kliknij Dalej.

4. Zostaniesz przekierowany do sekcji Logowanie; pozostaw okno Maltego bez zmian i kliknij ikonę Firefox w górnej części okna, aby uruchomić przeglądarkę Firefox.

5. Pojawi się okno Firefoksa w adresie typu https://www.maltego.com/ceregistration i naciśnij Enter.

6. Pojawi się strona Zarejestruj konto Maltego CE, wprowadź swoje dane i potwierdź captcha, a następnie kliknij przycisk ZAREJESTRUJ SIĘ, aby zarejestrować konto i je aktywować.

Uwaga: Jeśli w dolnej części przeglądarki pojawi się powiadomienie o plikach cookie, kliknij Akceptuj.

7. Poczta wysłana! pojawi się powiadomienie, kliknij przycisk zamykania.

8. Teraz w oknie przeglądarki kliknij ikonę „+”, aby otworzyć nową kartę. Otwórz konto e-mail podane podczas rejestracji w kroku 6. Otwórz wiadomość od Maltego i kliknij w link aktywacyjny.

9. Konto pomyślnie aktywowane! pojawi się strona, jak pokazano na zrzucie ekranu.

10. Zminimalizuj przeglądarkę internetową i wróć do kreatora konfiguracji oraz wprowadź adres e-mail i hasło podane podczas rejestracji; rozwiąż captcha i kliknij Dalej.

11. Sekcja Wynik logowania wyświetla Twoje dane osobowe; Kliknij Następny.

12. Pojawi się sekcja Install Transforms, która zainstaluje elementy z wybranego serwera tansform. Pozostaw ustawienia domyślne i kliknij Dalej

13. Pojawi się sekcja Pomóż ulepszyć Maltego. Pozostaw opcje ustawione na domyślne i kliknij Dalej

14. Zostanie wyświetlona sekcja Opcje przeglądarki internetowej. Pozostaw opcje ustawione na domyślne i kliknij Dalej.

15. Zostanie wyświetlona sekcja Opcje trybu prywatności. Pozostaw opcje ustawione na domyślne i kliknij Dalej.

16. Pojawi się sekcja Reasy, wybierz Otwórz pusty wykres i pozwól mi pobawić się opcjami i kliknij Zakończ

17. Pojawi się GUI Maltego Community Edition wraz z Powiadomieniem o zmianie polityki prywatności , kliknij przycisk Potwierdź.

18. Okno Maltego Community Edition wraz z oknem New Graph (1).

19. W lewym panelu Maltego GUI możesz znaleźć pole Entity Palette, które zawiera listę domyślnych wbudowanych transformacji. W węźle Infrastruktura w obszarze Paleta jednostek obserwuj listę jednostek, takich jak AS, nazwa DNS, domena, adres IPv4, adres URL, witryna internetowa itp.

20. Przeciągnij obiekt Witryna internetowa do okna Nowy wykres (1).

21. Jednostka pojawi się na nowym wykresie z domyślnie wybranym adresem URL www.paterva.com.

Uwaga: Jeśli nie możesz zobaczyć encji tak, jak pokazano na zrzucie ekranu, kliknij w oknie New Graph (1) i przewiń w górę, co zwiększy rozmiar encji.

22. Kliknij dwukrotnie nazwę www.paterva.com i zmień nazwę domeny na www.certifiedhacker.com; naciśnij enter.

23. Kliknij prawym przyciskiem myszy obiekt i wybierz opcję Wszystkie przekształcenia.

24. Pojawi się lista Run Transform(s); kliknij Do Domen [DNS].

25. Zostanie wyświetlona domena odpowiadająca witrynie.

26. Kliknij prawym przyciskiem myszy podmiot Certifiedhacker.com i wybierz Wszystkie transformacje -> Do nazwy DNS [Using Name Schema diction …]

27. Obserwuj stan na pasku postępu. Ta transformacja spróbuje przetestować różne schematy nazw w domenie i spróbuje zidentyfikować określony schemat nazw dla domeny,

28. Po zidentyfikowaniu schematu nazw osoby atakujące próbują symulować różne techniki wykorzystania, aby uzyskać poufne informacje dotyczące wynikowych schematów nazw. Na przykład osoba atakująca może przeprowadzić atak siłowy lub słownikowy w celu zalogowania się na stronie ftp.certifiedhacker.com i uzyskania poufnych informacji.

29. Wybierz tylko schematy nazw, przeciągając je i usuwając.

30. Kliknij prawym przyciskiem myszy podmiot Certifiedhacker.com i wybierz Wszystkie transformacje --> Do nazwy DNS — SOA (początek uprawnień).

31. Spowoduje to zwrócenie podstawowego serwera nazw i adresu e-mail administratora domeny, jak pokazano na poniższym zrzucie ekranu.

32. Wydobywając informacje związane z architekturą SOA, osoby atakujące próbują znaleźć luki w swoich usługach i architekturach oraz wykorzystać je.

33. Wybierz zarówno serwer nazw, jak i wiadomość e-mail, przeciągając je i usuwając.

34. Kliknij prawym przyciskiem myszy jednostkę Certifiedhacker.com i wybierz Wszystkie transformacje --> Do nazwy DNS - MX (serwer pocztowy).

35. Ta transformacja zwraca serwer pocztowy powiązany z domeną Certifiedhacer.com

36. Identyfikując serwer wymiany poczty, osoby atakujące próbują wykorzystać luki w zabezpieczeniach serwera, a tym samym wykorzystać go do wykonywania złośliwych działań, takich jak seding spam e-mail

37. Wybierz tylko serwer pocztowy, przeciągając go

38. Kliknij prawym przyciskiem myszy podmiot Certifiedhacker.com i wybierz Wszystkie transformacje -> Do nazwy DNS – NS (serwer nazw)

39. Spowoduje to zwrócenie serwerów nazw powiązanych z domeną, jak pokazano na poniższym zrzucie ekranu.

40. Identyfikując główny serwer nazw, osoba atakująca może zastosować różne techniki wykorzystania serwera, a tym samym wykonać złośliwe działania, takie jak przejęcie DNS i przekierowanie adresu URL.

41. Wybierz zarówno domenę, jak i serwer nazw, przeciągając je i usuwając.

42. Kliknij prawym przyciskiem myszy jednostkę i wybierz Wszystkie transformacje --> Do adresu IP [DNS].

43. Spowoduje to wyświetlenie adresu IP witryny internetowej, jak pokazano na poniższym zrzucie ekranu.

44. Uzyskując adres IP strony internetowej, osoba atakująca może symulować różne techniki skanowania w celu znalezienia otwartych portów i luk w zabezpieczeniach, a tym samym podjąć próbę wtargnięcia do sieci i wykorzystania ich.

45. Kliknij prawym przyciskiem myszy adres IP i wybierz Wszystkie przekształcenia --> Do lokalizacji [miasto, kraj].

46. Ta transformacja identyfikuje położenie geograficzne adresu IP, jak pokazano na poniższym zrzucie ekranu.

47. Uzyskując informacje związane z położeniem geograficznym, osoby atakujące mogą przeprowadzać ataki socjotechniczne, wykonując połączenia głosowe (vishing) z osobą fizyczną w celu wykorzystania poufnych informacji.

48. Teraz kliknij prawym przyciskiem myszy witrynę www.certifiedhacker.com i wybierz Wszystkie transformacje --> Do domen [DNS]. Domeny odpowiadające witrynie zostaną wyświetlone, jak pokazano na zrzucie ekranu.

49. Kliknij prawym przyciskiem myszy jednostkę domeny (certifiedhacker.com) i wybierz All Transform --> To Entities from WHOIS [IBM Watson].

50. Ta transformacja zwraca jednostki odnoszące się do właściciela domeny

51. Uzyskując te informacje, możesz wykorzystać serwery wyświetlone w wyniku lub zasymulować atak siłowy lub inną technikę włamania się na konto pocztowe administratora i wysyłania e-maili phishingowych do kontaktów na tym koncie.

52. Oprócz wyżej wymienionych metod, możesz wykonać footprinting na krytycznym pracowniku z docelowej organizacji, aby zebrać dodatkowe dane osobowe, takie jak adresy e-mail, numery telefonów, dane osobowe, wizerunek, alias, frazę itp.

53. W lewym okienku GUI Maltego kliknij węzeł Osobisty pod Paletą encji, aby obserwować listę encji, takich jak adres e-mail, numery telefonów, obraz, alias, fraza itp.

54. Poza wyżej wymienionymi transformatami, inne transformaty mogą śledzić konta i rozmowy osób zarejestrowanych na portalach społecznościowych, takich jak Twitter. Wyodrębnij wszystkie możliwe informacje.

55. Wydobywając wszystkie te informacje, możesz symulować działania, takie jak wyliczanie, hakowanie aplikacji internetowych, socjotechnika itp., które mogą umożliwić ci dostęp do systemu lub sieci, uzyskanie poświadczeń itp.

56. To kończy demonstrację odciskania stopy na celu za pomocą Maltego.

57. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 3: Określanie śladu celu za pomocą OSRFramework

OSRFramework to zestaw bibliotek używanych do wykonywania zadań Open Source Intelligence. Zawierają odniesienia do wielu różnych aplikacji związanych ze sprawdzaniem nazwy użytkownika, wyszukiwaniem DNS, badaniem wycieków informacji, głębokim wyszukiwaniem w sieci, ekstrakcją wyrażeń regularnych i wieloma innymi. Zapewnia również sposób graficznego tworzenia tych zapytań, a także kilka interfejsów do interakcji, takich jak OSRFConsole lub interfejs sieciowy.

1. Na maszynie wirtualnej Parrot Security. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

2. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

3. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter. Uwaga: Wpisane hasło nie będzie widoczne.

4. Teraz wpisz cd i naciśnij Enter, aby przejść do katalogu głównego.

5. Użyj domainfy, aby sprawdzić istniejące domeny za pomocą słów i pseudonimów. Wpisz domainfy -n [Nazwa domeny] -t all (tutaj docelową nazwą domeny jest ECCOUNCIL) i naciśnij Enter.

Uwaga: -n: określa pseudonim lub listę pseudonimów do sprawdzenia, -t: określa listę domen najwyższego poziomu, w których będzie wyszukiwany pseudonim.

6. Narzędzie pobierze wszystkie domeny wraz z ich adresami IP związanymi z domeną docelową. Korzystając z tych informacji, atakujący mogą dalej znajdować luki w subdomenach docelowej witryny i przeprowadzać ataki na aplikacje internetowe.

7. Użyj searchfy, aby sprawdzić, czy dane danego użytkownika istnieją na różnych platformach społecznościowych, takich jak Github, Instagram i Keyserverubuntu. Wpisz searchfy –q „docelowa nazwa użytkownika lub nazwa profilu” (tutaj docelowa nazwa użytkownika lub profil to Tim Cook i jest wyszukiwana na wszystkich platformach społecznościowych) i naciśnij Enter.

Uwaga: -q: określa zapytanie lub listę zapytań do wykonania.

8. Wyszukiwarka przeszuka dane użytkownika na platformach społecznościowych i poda informacje o istnieniu użytkownika. Te linki profilowe docelowego użytkownika mogą zostać wykorzystane przez osoby atakujące do przeprowadzenia ataków socjotechnicznych.

9. Podobnie możesz użyć następujących pakietów OSRFramework, aby zebrać więcej informacji o celu:

usufy - Gromadzi zarejestrowane konta z podanymi nazwami użytkowników.

mailfy — Zbiera informacje o kontach e-mail

phonefy - Sprawdza istnienie danej serii telefonów

entity — Wyodrębnia jednostki za pomocą wyrażeń regularnych z podanych adresów URL

10. Na tym kończy się demonstracja zbierania informacji o aliasach użytkowników docelowych z wielu platform mediów społecznościowych przy użyciu OSRFramework.

11. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

Zadanie 4: Ślad celu przy użyciu FOCA

FOCA (Fingerprinting Organizations with Collected Archives) to narzędzie, które ujawnia metadane i ukryte informacje w zeskanowanych dokumentach. Dokumenty te są wyszukiwane za pomocą trzech wyszukiwarek: Google, Bing i DuckDuckGo. Wyniki z trzech silników składają się na wiele dokumentów. FOCA bada szeroką gamę dokumentów, z których najbardziej rozpoznawalnymi są dokumenty Microsoft Office, Open Office i PDF. Może również współpracować z plikami Adobe InDesign lub SVG. Archiwa te mogą znajdować się na stronach internetowych i można je pobrać i przeanalizować za pomocą FOCA.

1. Włącz maszyny wirtualne Windows 11 i Windows Server 2019.

2. Na maszynach wirtualnych Windows Server 2019 kliknij Ctrl+Alt+Del, aby aktywować maszynę. Domyślnie wybrany jest profil użytkownika Administrator, wpisz Pa$$wOrd w polu Hasło i naciśnij Enter, aby się zalogować.

Uwaga: Pojawi się ekran Sieci. Kliknij Tak, aby komputer mógł być wykrywany przez inne komputery i urządzenia w sieci.

3. Aby uruchomić FOCA, przejdź do Z:\CEHvl2 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA i kliknij dwukrotnie plik FOCA.exe.

4. Pojawi się okno dialogowe FOCA, poczekaj na zakończenie inicjalizacji.

5. Pojawi się główne okno FOCA

6. Utwórz nowy projekt, przechodząc do Projektu i klikając Nowy projekt na pasku menu.

7. Pojawi się kreator nowego projektu FOCA, wykonaj poniższe czynności:

* Wprowadź nazwę projektu w polu Nazwa projektu (tutaj Projekt www.eccouncil.org).

* Wprowadź witrynę domeny w polu Witryna domeny (tutaj www.eccouncil.org).

* Opcjonalne pole Alternatywne domeny możesz pozostawić puste.

* W polu Folder, w którym chcesz zapisywać dokumenty, kliknij ikonę folderu. Kiedy pojawi się wyskakujące okienko Przeglądaj w poszukiwaniu folderu, wybierz lokalizację, w której chcesz zapisać dokument wyodrębniony przez FOCA (tutaj Pulpit) i kliknij OK.

* Pozostaw inne ustawienia domyślne i kliknij przycisk Utwórz.

8. Pojawi się wyskakujące okienko Projekt zapisany pomyślnie. Kliknij OK, aby je zamknąć.

9. Aby wyodrębnić informacje o docelowej domenie, wybierz wszystkie trzy wyszukiwarki (Google, Bing i DuckDuckGo) obecne w sekcji Wyszukiwarki. Podobnie w sekcji Rozszerzenia kliknij opcję Wszystkie, aby wybrać wszystkie podane rozszerzenia, a następnie kliknij przycisk Wyszukaj wszystko.

10. Przycisk Wyszukaj wszystko automatycznie przełącza przycisk Zatrzymaj i rozpoczyna zbieranie informacji o domenie docelowej w środkowym okienku.

11. Po zakończeniu skanowania przycisk Zatrzymaj automatycznie przełącza się z powrotem w przycisk Wyszukaj wszystko. Pojawi się zebrany wynik dotyczący metadanych powiązanych z domeną docelową, jak pokazano na zrzucie ekranu

12. Aby wyświetlić informacje o pliku przechowywane w subdomenie, kliknij prawym przyciskiem myszy dowolny adres URL i kliknij Link(i) --> Otwórz w przeglądarce z menu kontekstowego.

Uwaga: Jeśli pytanie Jak chcesz to otworzyć? pojawi się wyskakujące okienko, wybierz dowolną przeglądarkę internetową (tutaj Google Chrome) i kliknij OK.

13. Wyodrębniony plik z domeny za pomocą FOCA pojawia się w przeglądarce internetowej, jak pokazano na zrzucie ekranu.

14. Zamknij przeglądarkę internetową.

15. Wróć do okna FOCA i kliknij węzeł Sieć, aby rozwinąć węzeł w lewym panelu okna i wyświetlić strukturę sieci.

Uwaga: Używana przez nas domena nie ma powiązanych klientów ani serwerów.

16. Jeśli domena ma powiązanych klientów lub serwery, wyświetla powiązane informacje.

17. Rozwiń węzeł Domeny i kliknij domenę docelową (tutaj eccouncil.org), aby wyświetlić informacje związane z domeną.

18. w prawym okienku kliknij kartę Indeksowanie, a następnie kliknij przycisk indeksowania Google.

19. Funkcja indeksowania Google rozpoczyna indeksowanie witryny docelowej. Po zakończeniu indeksowania wyniki pojawią się w dolnym okienku.

20. Wyniki obejmują domeny uzyskane w wyniku skanowania wraz z ich ważnością, która jest wyświetlana jako niska, średnia lub wysoka, jak pokazano na zrzucie ekranu. Korzystając z tych informacji, osoby atakujące mogą dalej znajdować luki w domenie docelowej i wykorzystywać je do przeprowadzania ataków na aplikacje internetowe.

21. Teraz rozwiń węzeł Analiza dokumentów; dalej rozwiń węzeł Podsumowanie metadanych. Tutaj wyświetlane są informacje dotyczące użytkowników, folderów, drukarek, oprogramowania itp.

Uwaga: używana przez nas domena nie zawiera informacji powiązanych z podsumowaniem metadanych.

22. Na tym kończy się demonstracja zbierania przydatnych informacji o organizacji docelowej za pomocą narzędzia FOCA.

23. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

24. Wyłącz maszynę wirtualną Windows Server 2019.

Zadanie 5: Ślad celu przy użyciu BillCipher

BillCipher to narzędzie do zbierania informacji o stronie internetowej lub adresie IP. Za pomocą tego narzędzia możesz zbierać informacje, takie jak wyszukiwanie DNS, wyszukiwanie Whois, wyszukiwanie GeolP, wyszukiwanie podsieci, skaner portów, łącza do stron, transfer strefy, nagłówek HTTP itp. W tym przypadku użyjemy narzędzia BillCipher do śledzenia docelowego adresu URL witryny .

Uwaga: W tym przypadku za witrynę docelową uznamy witrynę www.certifiedhacker.com. Możesz jednak wybrać domenę docelową według własnego uznania.

1. Przełącz się na maszynę wirtualną Parrot Security. Kliknij ikonę terminala MATE w lewym górnym rogu pulpitu, aby otworzyć okno terminala.

2. Pojawi się okno Parrot Terminal. W oknie terminala wpisz sudo su i naciśnij Enter, aby uruchomić programy jako użytkownik root.

3. W polu [sudo] hasło atakującego wpisz toor jako hasło i naciśnij Enter.

Uwaga: Wpisane hasło nie będzie widoczne.

4. W oknie Parrot Terminal wpisz cd BillCipher i naciśnij Enter, aby przejść do Katalogu BillCipher.

5. Teraz wpisz python3 billcipher.py i naciśnij Enter, aby uruchomić aplikację.

6. Inicjalizacja aplikacji BillCipher. W polu Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? opcję, wpisz witryna i naciśnij Enter.

7. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

8. BillCipher wyświetla różne dostępne opcje, których możesz użyć do zebrania informacji dotyczących docelowej strony internetowej.

9. W oknie Jakie informacje chcesz zebrać? opcji, wpisz 1, aby wybrać opcję Wyszukiwanie DNS i naciśnij Enter.

10. Pojawi się wynik, wyświetlający informacje DNS dotyczące docelowej witryny, jak pokazano na zrzucie ekranu.

11. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

12. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

13. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

14. Teraz wpisz 3 i naciśnij Enter, aby wybrać opcję GeoIP Lookup z dostępnych opcji zbierania informacji.

15. Pojawi się wynik, wyświetlający informacje GeoIP Lookup docelowej witryny, jak pokazano na zrzucie ekranu.

16. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

17. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

18. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

19. Teraz wpisz 4 i naciśnij Enter, aby wybrać opcję Subnet Lookup spośród dostępnych opcji zbierania informacji.

20. Pojawi się wynik, wyświetlając informacje wyszukiwania podsieci docelowej witryny internetowej.

21. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

22. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

23. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

24. Teraz wpisz 6 i naciśnij Enter, aby wybrać opcję Linki do stron z dostępnych opcji gromadzenia informacji.

25. Pojawi się wynik, wyświetlając listę Widocznych łączy i Ukrytych łączy celu na stronie internetowej.

26. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

27. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

28. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

29. Teraz wpisz 8 i naciśnij Enter, aby wybrać opcję Nagłówek HTTP z dostępnych opcji zbierania informacji.

30. Pojawi się wynik, wyświetlający informacje dotyczące nagłówka HTTP docelowej witryny, jak pokazano na zrzucie ekranu.

31. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

32. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

33. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

34. Teraz wpisz 9 i naciśnij Enter, aby wybrać opcję Host Finder z dostępnej opcji zbierania informacji.

35. Pojawi się wynik, wyświetlający informacje dotyczące adresu IP docelowej witryny.3

36. W oknie Czy chcesz kontynuować? opcję, wpisz Tak i naciśnij Enter, aby kontynuować.

37. Czy chcesz zbierać informacje o stronie internetowej lub adresie IP? pojawi się opcja, wpisz stronę internetową i naciśnij Enter.

38. W opcji Wprowadź adres strony internetowej wpisz adres URL docelowej strony internetowej (tutaj www.certifiedhacker.com) i naciśnij Enter.

39. Teraz wpisz 19 i naciśnij Enter, aby wybrać opcję Kopiarka stron internetowych (użyj httrack) z dostępnych opcji zbierania informacji.

40. Narzędzie zaczyna odzwierciedlać docelową witrynę; zajmie to około 5 minut.

41. Po zakończeniu procesu tworzenia kopii lustrzanej witryna internetowa zostanie zapisana w folderze websource.

42. W oknie Czy chcesz kontynuować? opcji, wpisz No i naciśnij Enter, aby wyjść z BillCiper.

43. Teraz kliknij Miejsca w górnej części pulpitu i kliknij Folder domowy z menu kontekstowego.

44. Pojawi się okno atakującego, przejdź do BillCipher --> websource www.certifiedhacker.com --> www.certifiedhacker.com. Kliknij prawym przyciskiem myszy plik index.html i przejdź do Otwórz za pomocą --> Firefox, aby otworzyć lustrzaną witrynę.

45. Docelowa witryna lustrzana (www.certifiedhacker.com) pojawia się w przeglądarce Mozilla Firefox, jak pokazano na zrzucie ekranu.

46. Podobnie możesz użyć innych opcji zbierania informacji, aby zebrać informacje o celu.

47. To kończy demonstrację śledzenia docelowego adresu URL witryny za pomocą BillCipher.

48. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

49. Wyłącz maszynę wirtualną Parrot Security.

Zadanie 6: Footprinting celu przy użyciu OSINT Framework

OSiNT Framework to platforma gromadzenia danych wywiadowczych o otwartym kodzie źródłowym, która pomaga specjalistom ds. Koncentruje się na zbieraniu informacji z bezpłatnych narzędzi lub zasobów. Ta struktura zawiera prosty interfejs sieciowy, który zawiera listę różnych narzędzi OSINT uporządkowanych według kategorii i jest pokazany jako struktura drzewa OSINT w interfejsie sieciowym. OSINT Framework zawiera następujące wskaźniki wraz z dostępnymi narzędziami:

• (T) - wskazuje łącze do narzędzia, które należy zainstalować i uruchomić lokalnie

* (D) - Google Dork

• (R) - Wymaga rejestracji

• (M) - wskazuje adres URL, który zawiera wyszukiwane hasło, a sam adres URL należy edytować ręcznie

Tutaj użyjemy OSINT Framework do zbadania kategorii footprintów i powiązanych narzędzi.

1. Przełącz się na maszynę wirtualną Windows 11.

2. Otwórz dowolną przeglądarkę internetową (tutaj Mozilla Firefox). W pasku adresu przeglądarki umieść kursor myszy, wpisz https://osintframework.com/ i naciśnij Enter.

3. Pojawia się strona internetowa OSINT Framework; możesz obserwować drzewo OSINT po lewej stronie ekranu, jak pokazano na zrzucie ekranu.

4. Kliknięcie dowolnej kategorii, takiej jak nazwa użytkownika, adres e-mail lub nazwa domeny, spowoduje wyświetlenie wielu przydatnych zasobów na ekranie w postaci poddrzewa.

5. Kliknij kategorię Nazwa użytkownika i kliknij, aby rozwinąć podkategorie Wyszukiwarki nazw użytkowników i Określone witryny.

6. Możesz zobaczyć listę narzędzi OSINT przefiltrowaną według podkategorii (podkategorie Wyszukiwarki nazw użytkowników i Podkategorie określonych witryn).

7. Na liście dostępnych narzędzi w kategorii Wyszukiwarki nazw użytkowników kliknij narzędzie NameCheckr, aby przejść do witryny NameCheckr.

8. Pojawi się witryna NameCheckr, jak pokazano na zrzucie ekranu.

9. Zamknij bieżącą kartę, aby wrócić do strony WWW OSINT Framework.

10. Podobnie możesz przeglądać inne narzędzia z listy wspomnianych narzędzi w podkategoriach Wyszukiwarki nazw użytkowników i Określone witryny.

11. Teraz kliknij kategorię Nazwa domeny, a pojawią się jej podkategorie. Kliknij, aby rozwinąć podkategorię Whois Records.

12. Pojawi się lista narzędzi w podkategorii Whois Records; kliknij narzędzie Dossier domeny.

13. Zostanie wyświetlona witryna Domain Dossier, jak pokazano na zrzucie ekranu.

Uwaga: narzędzie Domain Dossier generuje raporty z publicznych rejestrów dotyczące nazw domen i adresów IP, aby pomóc w rozwiązywaniu problemów, badaniu cyberprzestępczości lub po prostu lepiej zrozumieć, jak wszystko jest skonfigurowane.

14. Zamknij bieżącą kartę, aby wrócić do strony WWW OSINT Framework.

15. Teraz kliknij kategorię Metadane i kliknij narzędzie FOCA z listy dostępnych narzędzi.

16. Pojawi się strona internetowa FOCA, wyświetlająca informacje o narzędziu wraz z linkiem do jego pobrania, jak pokazano na zrzucie ekranu.

17. Podobnie możesz przeglądać inne dostępne kategorie, takie jak adres e-mail, adres IP, sieci społecznościowe, komunikatory itp. oraz narzędzia powiązane z każdą kategorią. Korzystając z tych narzędzi, możesz wykonać footprinting w organizacji docelowej.

18. To kończy demonstrację wykonywania footprintingu przy użyciu OSINT Framework.

19. Możesz także użyć narzędzi do śledzenia śladów, takich jak Recon-Dog (https://www.github.com), Grecon (https://github.com), Th3lnspector (https://github.com), Raccoon (https ://github.com), Orb (https://github.com) itp. w celu zebrania dodatkowych informacji związanych z przejmowaną spółką.

20. Zamknij wszystkie otwarte okna i udokumentuj wszystkie uzyskane informacje.

21. Wyłącz maszynę wirtualną Windows 11.