POI

Nazwisko: _____
Rok/grupa: _____

Ćwiczenie laboratoryjne V
Cain&Abel – narzędzie do penetrowania systemów komputerowych i ich zabezpieczeń

To jest laboratorium ćwiczeniowe. Należy jest wykonać w czasie trwania zajęć. Zadanie to nie powinno zająć więcej czasu niż czas trwania laboratorium. Jeśli zadanie zostanie zakończone wcześniej, to można kontynuować prace dotyczące poprzedniego laboratorium lub pracy semestralnej.

Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z podstawowym narzędziem do odzyskiwania różnych typów haseł przez podsłuchiwanie sieci, łamanie zaszyfrowanych haseł atakami siłowymi, słownikowymi lub kryptoanalitycznymi, nagrywanie rozmów VoIP, odzyskiwanie kluczy sieci bezprzewodowych, odkrywanie haseł z pamięci cache i analizowanie protokołów sieciowych

Efekty

Po ukończeniu ćwiczenia studenci powinni posiadać wystarczającą wiedzę dotyczącą łamania i odzyskiwania haseł. Uzyskują także podstawową wiedzę na temat sprawdzania zabezpieczeń systemów komputerowych.

1. Wstęp

Cain & Abel został zaprojektowany z myślą o administratorach sieci, nauczycielach, specjalistów od zabezpieczeń, biegłych sądowych, testerach penetracyjnych i innych którzy potrzebowaliby tego programu do etycznych celów. Niemniej należy pamiętać, że używając tego programu można spowodować zniszczenie lub utratę danych.

Cain & Abel to tak naprawdę dwa programy. Pierwszy, Cain zawiera graficzny interfejs użytkownika. Za jego pomocą korzysta się z większości funkcjonalności. Abel jest natomiast usługą NT składającą się z dwóch plików: „Abel.exe” oraz „Abel.dll”. Te pliki są kopiowane przez instalatora do ścieżki podanej przez użytkownika, ale Abel nie jest instalowany. Można to zrobić lokalnie lub zdalnie (używając Caina) pod warunkiem, że posiada się prawa Administratora.

Główną funkcjonalnością Abla jest dostęp do konsoli na hoście, na którym Abel jest zainstalowany. Poza tym potrafi zrzucić skróty z haseł użytkowników z bazy danych SAM (Security Accounts Manager) nawet jeśli zostały zaszyfrowane narzędziem „Syskey". Udostępnia też takie funkcjonalności jak dostęp do sekretów LSA z rejestru.

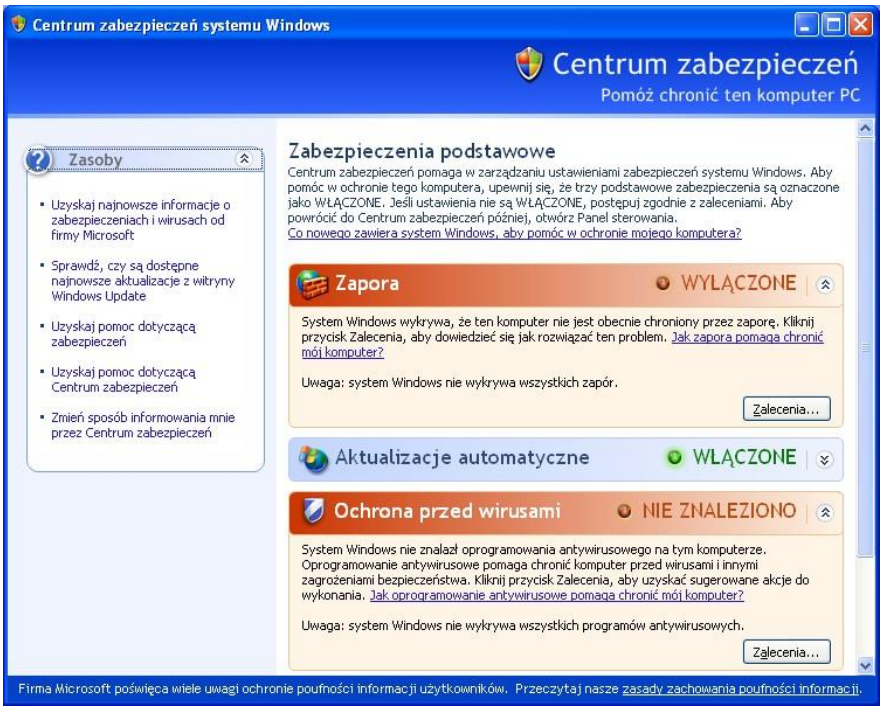
Funkcjonalność Caina składa się z następujących elementów:

- Manager przechowywanych haseł – odczytuje hasła lokalnie przechowywane w Outlooku, Internet Explorerze i MNS Explorerze (http://www.mediacollege.com/microsoft/internet-explorer/6/autocomplete.html)
- Manager dekodera haseł – odczytuje hasła przechowywane w Enterprise and Local Credential Sets na windows XP/2003
- LSA Secret Dumper – zrzuca zawartość LSA (sekrety).
- Dekoder haseł Dialup – odczytuje hasła przechowywane przez Windows w DialUp |Networking
- APR (ARP Poison Routing) – włącza nasłuchiwanie w sieci komputerowej i pozwala na ataki typu „man in the middle"
- Manager tablicy routingu – dostarcza tę samą funkcjonalność co windowsowe polecenie „route", ale z interfejsem GUI
- Skaner SID – Wyciąga nazwę użytkownika powiązaną z Identyfikatorem bezpieczeństwa (SID) na zdalnym systemie
- Network Enumerator – odczytuje (gdzie jest to możliwe) nazwy użytkowników, grup, danych dzielonych (shares) oraz usług działających na maszynie
- Rejestr zdalny – pozwala na modyfikację parametrów w rejestrze z sieci
- Manager Usług – pozwala na zatrzymanie, wystartowanie, wykonanie pauzy lub zezwolenie na dalsze wykonywanie usługi (continue) lub usunięcie usługi
- Sniffer – pozwala przechwytywać hasła, hashe, i inne informacje weryfikujące użytkownika podczas ich transmisji przez sieć. Zawiera różne filtry, np. VoIP. Routing Protocol Monitors – monitoruje wiadomości przesyłane za pomocą różnych protokołów w celu przechwycenia danych weryfikacyjnych i dzielonych tablic routingu.
- Pełny sniffer do ARP dla różnych protokołów: RDP, SSH-1, HTTPS, FTPS, POP3, IMAPS, LDAPS. Sniffer ten pozwala na przechwycenie wszystkich danych przesyłanych konkretnym protokołem.
- Collector certyfikatów – zbiera przesyłane certyfikaty

2. Podstawy korzystania z Abla

Abla można zainstalować na dowolnym komputerze do którego posiada się uprawnienia Administratora, w tym również na localhost. Najłatwiej w ten sposób zapoznać z jego możliwościami bez konieczności łączenia się z jakąkolwiek siecią.

Uwaga. Przed uruchomieniem programu Cain & Abel należy wyłączyć zaporę systemu Windows (patrz rysunek poniżej). W przeciwnym przypadku nie będą poprawnie działały niektóre zaawansowane opcje programu Cain & Abel.



Zadanie 1: zainstaluj Abla na swoim komputerze.

1. Wybierz zakładkę „Network” w Cainie
2. Kliknij PPM na Quick List
3. Wybierz „Add to quick list”
4. Wpisz „127.0.0.1” (bez cudzysłowiu) i zatwierdź
5. Na nowo dodanym elemencie szybko kliknij dwa razy
6. Rozwiń listę, aby zlokalizować pozycję „Services”
7. Kliknij na nią PPM i wybierz „Install Abel”

Pytanie 1: Jakie są tam widoczne pozycje oprócz „Services”? Co pozwalają zrobić? Gratulacje! Usługa Abla została skopiowana i uruchomiona na docelowym hoście.

Powinna być widoczna na szczycie listy wszystkich uruchomionych aktualnie usług. Jeśli jesteś na Win7, możesz spróbować wyłączyć na chwilę usługę *Themes,* żeby zobaczyć swój wpływ na zainfekowany system.

Mimo, że Abel działa, Cain aktualnie wyświetla te same dane jak przed instalacją. Aby zacząć korzystać z Abla, należy rozłączyć się z zainfekowanym systemem i połączyć ponownie. Nad identyfikatorem użytkownika pojawi się nowa rozwijana pozycja: „Abel".

Konsola. Daje możliwość dostępu do konsoli tak jak uruchomionej lokalnie. Na początku jest domyślnie ustawiona na katalog *C:\Windows\system32*.

Zadanie 2: Za pomocą konsoli, stwórz nowy folder na dysku C:\ swojego komputera.

1. cd C:\
2. mkdir IMAT00L
3. Sprawdź, czy nowy folder pojawił się na dysku C

Hashes. Pobiera skróty haseł dla wszystkich użytkowników systemu. Można je wysłać do Crackera, aby je odzyskać.

LSA Secrets. Pobiera sekrety LSA. Więcej na ten temat w rozdz. nastepnym.

3. Sekrety LSA

Sekrety LSA to specjalna chroniona przestrzeń na ważne dane używane przez Local Security Authority. LSA jest przeznaczony do zarządzania systemowymi lokalnymi politykami bezpieczeństwa, przeprowadzania audytów, uwierzytelniania, logowania użytkowników, przechowywania prywatnych danych. Dostęp do tej przestrzeni w teorii ma tylko system, ale mogą tam mieć dostęp też inne programy jak na przykład „Windows Password Recovery".

Sekrety LSA są zlokalizowane w HKEY_LOCAL_MACHINE\Security\Policy\Secrets i może zawierać hasła RAS/VPN, autologowania i inne systemowe hasła lub klucze.

Zadanie 3: włącz autologowanie i sprawdź hasło Cainem: Windows XP or 7:

1. Wciśnij klawisz Windows + R, pokaże Ci się okno "Uruchom…"
2. Wpisz "**control userpasswords2"** i potwierdź enterem. Pojawi się okno kont użytkowników.
3. Odznacz opcję "*Users must enter a user name and password to use this computer*"
4. Kliknij "OK". Zostaniesz poproszony o podanie hasła.

Jeżeli nie będzie tam wyświetlonego checkboxa z opcją z kroku (3), oznacza to, że jesteś zalogowany jako Administrator. Można to obejść zmieniając wartość rejestru *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows*

NT\CurrentVersion\Winlogon\AutoAdminLogon na 1. Lepiej jednak zrobić to na koncie innego użytkownika.

4. Hasła lokalnych użytkowników

NTLM (NT Lan Manager) – zestaw protokołów definiujących metody zapewniania autentykacji, integralności i poufności danych użytkowników. Zastąpił starszy produkt (Lan Manager, LM). NTLM nie jest już rekomendowany do użycia, ponieważ nie używa współczesnych metod kryptograficznych takich jak AES czy SHA-256 (na przykład szyfrowanie odbywa się przy użyciu RC4). Mimo to, Windowsy XP oraz 7 nadal przechowują skróty haseł lokalnych użytkowników wygenerowane przez narzędzia NTLM.

Cain pozwala szybko uzyskać te hashe, a także udostępnia narzędzia, które mogą pozwolić na odzyskanie na ich podstawie haseł.

Rodzaje ataków na hasło w Cain:

a) Pełny przegląd (brute-force) – polega na wygenerowaniu każdej możliwej kombinacji dozwolonych znaków. Skuteczny albo dla bardzo krótkich haseł, albo dla średnich, pod warunkiem, że liczba dozwolonych znaków jest niska. Mając nieograniczone zasoby czasowe, ten typ ataku zawsze się powiedzie.

b) Słownikowy (dictionary) – do jego wykonania potrzebna jest lista słów. Oprócz sprawdzenia tych słów, atak można poszerzyć przez generowanie wariantów słów w słowniku, na przykład: odwrócenie kolejności liter, dodanie jedynki na koniec, wygenerowanie wariantów z mieszanymi małymi i dużymi literami.

c) Tęczowe tablice (rainbow tables) – ta metoda jest stosowana tylko przy ataku na skrót z hasła. Atak opiera się na bazie wcześniej obliczonych skrótów z pewnej bazy haseł. Zazwyczaj tablice zajmują bardzo wiele miejsca, stosuje się je więc, gdy przestrzeń na dysku nie stanowi problemu, natomiast czas jest kluczowym zasobem – nie trzeba bowiem obliczać hashu przy każdym nowym wygenerowanym haśle, co normalnie następuje w dwóch atakach wymienionych powyżej.

Uwaga! Przed laboratorium ściągnij tęczową tablicę dla odpowiedniego systemu operacyjnego z http://ophcrack.sourceforge.net/tables.php

Zadanie 4: Stwórz trzech użytkowników „u1”, „u2” oraz „u3”. Ustaw hasła dla każdego konta odpowiednio na: „abc”, „bl00dstain”, „123pAsSwOrD321”

Pytanie 2: Jak bezpieczne są te hasła wg howsecureismypassword.net? Podaj kolor strony.

Zadanie 5: Wylistuj wszystkich lokalnych użytkowników w systemie

W programie Cain

1. Wybierz zakładka Cracker (czwarta od lewej)

---

2. W drzewiastym menu po lewej wybierz pierwszą pozycję od góry (LM & NTLM Hashes)
3. Kliknij „+” na pasku powyżej
4. W wyskakującym okienku wybierz „Import Hashes from local system” i kliknij „Next”

Pojawi się lista użytkowników w systemie. Te konta, na które można się zalogować (np. z powodu pustego hasła) będą miały ikonę klucza, pozostałe zaś czerwone krzyżyki.

W menu kontekstowym można rozpocząć ataki: brute-force, słownikowy, kryptoanalityczny. Po wyborze konkretnego ataku pojawi się okno w którym można ustawić parametry ataku.

Pytanie 3. Zmieniając parametry ataku siłowego, odczytaj ile czasu potrzebuje przeciętny komputer na złamanie

a) 6-znakowego hasła składającego się tylko z małych liter
b) 12-znakowego hasła składającego się tylko z małych liter
c) 6-znakowego hasła składającego się z małych i dużych liter
d) 12-znakowego hasła składającego się z małych i dużych liter
e) 6-znakowego hasła składającego się z cyfr, małych i dużych liter
f) 12-znakowego hasła składającego się z cyfr, małych i dużych liter

Zadanie 6. Złam hasła utworzonych przez siebie wcześniej użytkowników. Użyj ataku siłowego do złamania hasła „u1”, słownikowego do hasła „u2” oraz ataku kryptoanalitycznego z wykorzystaniem tablic OphCrack do hasła „u3”

5. Lokalnie przechowywane hasła

Protected Storage Password Manager pozwala na odczytywanie lokalnie przechowywanych haseł w Outlooku, Internet Explorerze i MNS Explorerze. Jest to możliwe dzięki części MicrosoftApi jakim jest Protected Store. Jest on głównie używany do przechowywania haseł używanych przez użytkownika. Wszystkie informacje przechowywane w Protected Store są zaszyfrowane za pomocą klucza tworzonego na podstawie głównego hasła do logowania danego użytkownika. Dostęp do tej informacji jest możliwy tylko przez właściciela. Tej funkcjonalności używa część programów Windowsowych takich jak: Outlook, MNS Explorer, Internet Explorer. Dane te są przechowywane w rejestrze po ścieżką:
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider.

Zanim zaczniesz zadanie upewnij się, że masz uprawnienia administratora. Wszystkie zadania możesz wykonywać na localhost.

Zadanie 7. Otwórz Internet Explorer. Poczekaj aż się załaduje, a potem wejdź na dowolną stronę z formularzem logowania (www.mail.com, www.poczta.onet.pl). Spróbuj się zalogować (możesz podać nieprawdziwe dane logowania), a gdy IE zapyta, czy zapamiętać hasło – zgódź się. Jeżeli nie zapyta, to oznacza że korzystasz z Internet Explorera 6. Wejdź w Tools -> Internet options -> Content -> Autocomplete i zaznacz wszystkie checkboxy.

W Cainie, wybierz pierwszą zakładkę (Decoders) a na liście po lewej stronie wybierz "IE7 Passwords". Kliknij na pustą przestrzeń po prawej stronie, a następnie na ikonę plusa powyżej.

6. ARP Route Poisoning/Spoofing

ARP (Address Resolution Protocol) to protokół wykorzystywany do tłumaczenia adresów warstwy sieciowej (adresy IP) na adresy warstwy łącza danych (adresy MAC). Określa sposób wymiany zdefiniowanych przez protokół pakietów oraz działanie jakie musi wykonywać system operacyjny, aby konwersja adresów była możliwa.

Zasada działania opiera się na tabeli przechowywanej przez system operacyjny. Gdy występuje potrzeba wysłania pakietu na adres MAC, którego nie ma w tabeli, do wszystkich hostów w podsieci jest wysyłane żądanie zawierające adres IP, który ma zostać przetłumaczony oraz adres MAC autora żądania. Protokół określa, że na takie żądanie odpowiedzieć (swoimi adresami IP i MAC) ma tylko ten host, który ma taki adres IP jaki został zawarty w żądaniu. Te dane zostają zapisane w tablicy, aby nie trzeba było wysyłać pakietów ARP przy każdej próbie konwersji adresów.

Atak ARP (ARP Route Poisoning) polega na rozsyłaniu spreparowanych (fałszywych) pakietów. Można w ten sposób wykonać atak „Man in the Middle" (MitM). Przyjmijmy następujący scenariusz: w sieci istnieje podmiot A, B oraz C – my. A komunikuje się z B. Jeżeli uda nam się wykonać atak ARP, to przedstawimy się podmiotowi A jako B, a podmiotowi B jako A. W ten sposób, jeżeli będą próbowali coś do siebie wysłać, wyślą to do podmiotu C – czyli do nas. Możemy wtedy monitorować ich komunikację.

Przeprowadzenie takiego ataku za pomocą Caina jest przerażająco proste. **Zadanie 8.**

1. W pierwszej kolejności należy sprawdzić jakie hosty są widoczne w naszej sieci.
2. Włącz Sniffera (druga ikona od lewej na górnym pasku)
3. Wybierz zakładkę „Sniffer"
4. Kliknij PPM i wybierz „Scan MAC Addresses" (w oknie które się pojawi kliknij OK)

Masz teraz przed sobą listę wszystkich urządzeń wraz z ich adresami MAC w Twojej podsieci. Można pobrać dla każdego z nich nazwę (przez zaznaczenie + PPM → Resolve Hostname), ale jest to dość kosztowna czasowo operacja.

Pytanie 4: Podaj numer IP, adres MAC oraz nazwę Twojego komputera. Podaj te same dane domyślnej bramy Twojej sieci (aby zidentyfikować adres IP bramy domyślnej, posłuż się poleceniem ipconfig).

Mamy już listę potencjalnych ofiar naszego ataku. Prawda jest taka, że przy normalnym użytkowaniu bardzo rzadko stacje z tej samej sieci komunikują się ze sobą (chyba, że w podsieci jest serwer udostępniający jakieś usługi). W związku z tym, zamiast atakować połączenie między dwoma stacjami, dokonamy ataku między stacją a jej bramą domyślną.

Zadanie 9. Wykonaj atak ARP

Uwaga. Do wykonania tego zadania wymagane są co najmniej dwie stacje robocze: atakującego i ofiary (trzeciej nie trzeba, bo brama domyślna zawsze będzie). Jeżeli wykonujesz to zadanie na maszynie wirtualnej, za ofiarę w zupełności może posłużyć host maszyny wirtualnej. Upewnij się tylko, że ustawienia sieciowe maszyny pozwalają widzieć się nawzajem obu systemom operacyjnym (W ustawieniach maszyny, zakładka *Network*: zaznaczy *Enable Network Adapter*, w *Attached to* wybierz *Bridged Adapter*). Jeżeli nie korzystasz z maszyny wirtualnej, wybierz stację roboczą, na której pracuje Twój przyjaciel.

1. W zakładce „Sniffer” wybierz na dole podzakładkę „ARP”
2. Kliknij na pustą listę w wyższej części okna. Plus (siódma ikona od lewej w górnym pasku) powinna się odszarzyć. Kliknij plusa.
3. W nowym okienku wybierz numer IP stacji atakowanej. Po prawej stronie wybierz numer IP bramy domyślnej, po czym kliknij OK.
4. W górnej liście powinien pojawić się nowy wpis. Kliknij „Start/Stop APR” (trzecia ikona od lewej w górnym pasku).
5. Dolna lista powinna zapełnić się wieloma połączeniam, które nawiązuje atakowany host.

Brawo! Właśnie skutecznie wykonałeś atak MItM! Czas wykorzystać to w celu odzyskania hasła.

Wybierz podzakładkę „Passwords” na dole okna Caina. Tutaj Cain wyświetla wszystkie pakiety danego rodzaju, które mogą nas zainteresować.

Kategoria HTTP będzie prawdopodobnie pogrubiona, co oznacza że zostały złapane pakiety mogące zawierać hasła. Wybierz ją. Przeglądając pakiety zwróć uwagę na kolumnę *„Client”* - duża część z nich może należeć do Twojej stacji roboczej, ponieważ podsłuchujesz cały ruch jaki przechodzi przez Twoją kartę sieciową – również Twoją internetową aktywność. Aby odróżnić pakiety pochodzące z Twojej stacji od pakietów z podsłuchiwanego hosta, posortuj je według kolumny „Client”.

Nie są tu wyświetlone wszystkie złapane pakiety – to mógłbyś osiągnąć innym narzędziem,

---

np. Wiershark lub po prostu tcpdump. Cain analizuje pakiety, wybiera te, które są zgodne z protokołem HTTP a następnie skanuje je pod względem pewnych słów kluczowych. Można je zobaczyć (i zmienić) klikając „*Configure*" w górnym pasku menu a następnie wybierając zakładkę „*HTTP Fields*". Jak widać, jest tam wiele wyrażeń, które popularnie używane są do nazywania formularzy podawania logina i hasła użytkowników. Konsekwencją takiej listy jest fakt, że wiele złapanych przez Caina pakietów i zatwierdzonych jako te przechowujące hasło jest tak naprawdę zupełnie nieistotnych z naszego punktu widzenia.

Jeżeli zależy nam na odzyskaniu hasła z konkretnego serwisu, możemy sprawdzić jak są nazywane w nim pola loginu i hasła i dodać je do listy analizowanych pól HTTP.

Pytanie 5: Jakie mają nazwy i identyfikatory pola wpisywania loginu i hasła w serwisie www.mail.com?

Zadanie 10. Odzyskaj hasło z podsłuchiwanej maszyny. W tym celu wejdź na zaatakowanej maszynie na www.mail.com i wpisz (dowolne) dane logowania. Cain powinien wychwycić te dane. Jeśli nie, upewnij się, że ikony sniffera oraz ataku ARP są wciśnięte.

Sprawozdanie z ćwiczenia

W trakcie ćwiczenia należy notować wszystkie czynności oraz uzyskiwane wyniki. Po zakończeniu ćwiczenia należy przygotować sprawozdanie z przebiegu ćwiczenia, zawierające m.in. krótki opis ćwiczenia, uzyskane wyniki oraz podsumowanie i wnioski z ćwiczenia.

Sprawozdanie powinno zawierać także odpowiedzi na wszystkie pytanie zadane w konspekcie.

Literatura

1. Strona http://www.oxid.it/cain.html