Social Engineering i Social Engeenering Toolkit

co to jest i jakie ma zastosowanie w praktyce

Ewa Śliwoń i Krzysztof Konieczny

7 lutego 2020

Co to jest Inżynieria Socjalna?

Inżynieria społeczna, inżynieria socjalna, socjotechnika (ang. social engineering) – w politologii, socjologii i marketingu: zespół technik służących osiągnięciu określonych celów poprzez manipulację społeczeństwem. Innymi słowy jest to celowe, przemyślane przekształcanie społeczeństwa. Stanowi jedną z najważniejszych form oddziaływania aparatu państwowego, partii politycznych i elity władzy na tych których:

- **już się kontroluje**
- **pragnie się kontrolować**
- **przeszkadzają w sprawowaniu kontroli**

Osoba posługująca się inżynierią społeczną sądzi, że cel, do którego dąży, jest ważniejszy niż prawda czy niezależność myślenia osób poddawanych manipulacji. **Socjotechnika** odwołuje się do **emocji człowieka** i stara się uśpić ludzki rozum. Często socjotechnik stara się przekonać odbiorcę jego przekazu do swoich idei nawet kosztem nieetycznego odrywania ich od rzeczywistości, bo sądzi on, że **"cel jego działalności uświęca takie środki".**

Stosowane Techniki

- **pozorny wybór** – adept socjotechniki przedstawia podmiotom manipulacji kilka punktów widzenia, ale zdanie zgodne z jego poglądami w zawoalowany sposób ukazuje w bardziej pozytywnych barwach
- **ośmieszanie** – manipulator stara się ośmieszyć nieodpowiadające mu idee
- **autorytatywne świadectwo** – socjotechnik powołuje się na powszechnie akceptowany autorytet
- **transfer (przeniesienie)** – osoba manipulująca społecznością stara się skojarzyć swoje przesłanie z pozytywnym pojęciem ugruntowanym wśród jego odbiorców, często poprzez tworzenie zbitek słownych
- **niezależne zdanie** – adept inżynierii społecznej tak kształtuje przekaz, aby stworzyć wrażenie, że nie zależy mu na przekonaniu odbiorców do swojego zdania

- **selekcja faktów** – manipulator wybiera fakty tylko dla niego wygodne i pozwala odbiorcom na dostęp tylko do jego przekazów
- **zamiana nazw (nowomowa)** – socjotechnik tworzy nowe pojęcie, któremu nadaje silne tło emocjonalne, a potem wykorzystuje je masowo w konstruowaniu komunikatów przekazywanych manipulowanym osobom
- **wskazywanie negatywnych grup odniesienia (wskazywanie wroga)** – manipulator wskazuje wroga, który ma zagrażać grupie odbiorców jego przekazu, co pozwala na jej konsolidację wokół promowanych przez niego idei
- **zdanie większości** – adept inżynierii społecznej twierdzi, że jego zdanie podziela większość i twierdzi, że wszyscy swoi tak mówią
- **tworzenie stereotypów** – osoba manipulująca grupą tworzy stereotyp, a potem stale go używa, aby wzmocnić jego siłę

- **kłamstwo** – socjotechnik kłamie, ale stara się uprawdopodobnić swoje twierdzenia i ogranicza dostęp odbiorcy do innych źródeł informacji, łączy kłamstwa z faktami
- **powtarzanie sloganów** – specjalista od socjotechniki wymyśla slogan, który stara się potem jak najbardziej rozpowszechnić
- **kształtowanie tła emocjonalnego** – osoba stosująca inżynierię społeczną stara się swój przekaz skojarzyć z elementami budzącymi pozytywne uczucia, poprzez tworzenie miłej atmosfery, czy pozytywnego tła

Psychotechnika a Socjotechnika

Psychotechnika to nauka praktyczna, która przy uwzględnieniu ocen i znajomości ogólnych prawidłowości psychicznych przez zalecenia odpowiednich środków będzie dążyć do uzyskania przewidzianych środków psychicznych u danej jednostki. Stosuje się ją tam, gdzie chodzi o uzyskanie zmiany w opiniach, postawach lub zachowaniach jednostki. Zmierza do zmienienia człowieka pod jakimś szczególnym względem lub do narzucenia mu pewnej określonej identyfikacji czy też zmiany uprzednio posiadanej identyfikacji.

Socjotechnika to taka nauka praktyczna, która przy uwzględnieniu uznawanych ocen oraz przy uwzględnieniu ogólnych prawidłowości społecznych dążyć będzie przy stosowaniu zalecanych środków do wywołania określonych skutków społecznych. Ma zastosowanie wtedy, gdy zmiana będzie dotyczyć opinii postaw i zachowań jednostki abstrakcyjnej, modelowej. Zdąża do ukształtowania łatwo społecznie rozprowadzalnego całościowego wzoru osobowego lub pewnego stereotypu zachowania częściowego.

Co to jest Social Engeenering Toolkit?

Social-Engineer Toolkit (SET) został specjalnie zaprojektowany do przeprowadzania zaawansowanych ataków na element ludzki. ZESTAW został zaprojektowany do wydania wraz z uruchomieniem **https://www.social-engineer.org** i szybko stał się standardowym narzędziem w arsenale testerów penetracyjnych. SET został napisany przez **Davida Kennedy'ego** i przy dużej pomocy społeczności wprowadził ataki, których nigdy wcześniej nie widziano w zestawie narzędzi wykorzystywania. Ataki wbudowane w zestaw narzędzi mają na celu ukierunkowane i ukierunkowane ataki na osobę lub organizację wykorzystane podczas testu penetracyjnego. Mózgiem SET jest **plik konfiguracyjny**. Domyślnie SET sprawdza się idealnie dla większości ludzi, jednak może być konieczne zaawansowane dostosowanie, aby upewnić się, że wektory ataku zostaną uruchomione bez żadnych problemów.

W jaki sposób możemy go skonfigurować?

- Pierwszą opcją jest zmiana ścieżki położenia Metasploit. **Metasploit** jest wykorzystywany do tworzenia ładunków, błędów formatu plików i sekcji wykorzystywania przeglądarki.
- **Sekcja Ettercap** może być używana, gdy jest się w tej samej podsieci co ofiary i chce się wykonywać ataki z użyciem DNS na podzbiór adresów IP. Gdy jest ustawiona na „ON”., zatruwa całą lokalną podsieć i przekierowuje określoną witrynę lub wszystkie witryny do uruchomionego złośliwego serwera.
- Ustawienie **SENDMAIL** na "ON" spowoduje uruchomienie SENDMAIL, który może sfałszować źródłowe adresy e-mail. Ten atak działa tylko wtedy, gdy serwer SMTP ofiary nie wykonuje wyszukiwania wstecznego na nazwie hosta. SENDMAIL musi być zainstalowany.
- Po ustawieniu **WEBATTACK EMAIL** na "ON", będzie można wysyłać masowe wiadomości e-mail do ofiary, korzystając z wektora "Web Attack".

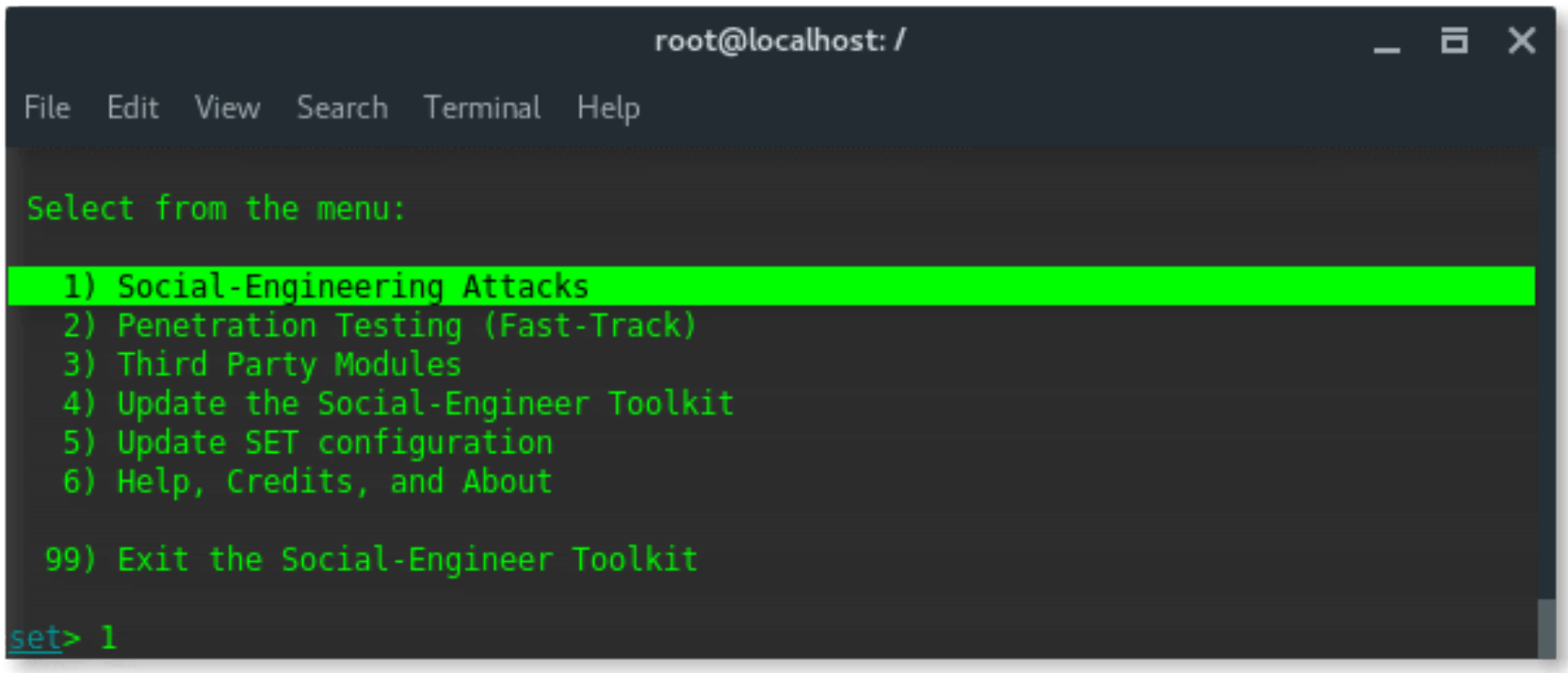
- **Wektor Java Applet Attack** to atak o jednym z najwyższych wskaźników sukcesu, jaki SET osiągnął w swoim arsenale. Aby wyglądał bardziej wiarygodnie, można włączyć tę opcję, która pozwoli nam podpisać Java Applet pod dowolną nazwą, a druga opcja zachęci użytkownika w kółko z dokuczliwymi ostrzeżeniami, jeśli anulują. Jest to przydatne, gdy użytkownik kliknie przycisk Anuluj, a atak stanie się bezużyteczny, zamiast tego będzie się pojawiał w kółko.
- Opcja **AUTO DETECT** jest prawdopodobnie jednym z najczęściej zadawanych pytań w SET. Jeśli zmieni się opcję na "OFF", SET wyświetli dodatkowe pytania dotyczące przygotowania ataku. Ta opcja powinna być używana, gdy chce się korzystać z wielu interfejsów, mieć zewnętrzny adres IP lub jesteś w scenariuszu przekierowania NAT / Port.

- W niektórych przypadkach, gdy przeprowadzamy zaawansowany atak inżyniera społecznościowego, możemy zarejestrować domenę i kupić certyfikat SSL, który sprawi, że atak będzie bardziej wiarygodny. Wówczas możemy włączyć ataki SSL za pomocą SET. Musimy jedynie włączyć **WEBATTACK SSL na "ON".** Jeśli chcemy skorzystać z certyfikatów z podpisem własnym, jednak gdy ofiara przejdzie na naszą stronę, pojawi się ostrzeżenie **„niezaufane”**.
- **Atak WebJacking** odbywa się poprzez zastąpienie przeglądarki ofiary innym oknem, które ma wyglądać i pojawiać jak legalna witryna. Ten atak jest bardzo zależny od czasu, jeśli robimy to przez Internet, zalecane opóźnienie powinno wynosić około 5000 (5 sekund).

- Funkcja **AUTO MIGRATE** automatycznie migruje do notatnika.exe, gdy pokaże się powłoka licznika. Jest to szczególnie przydatne podczas korzystania z exploitów **(program mający na celu wykorzystanie błędów w oprogramowaniu)** przeglądarki, ponieważ zakończy sesję, jeśli przeglądarka zostanie zamknięta podczas korzystania z exploita.
- **Metoda kradzieży podpisu cyfrowego** wymaga modułu python o nazwie PEFILE, który wykorzystuje technikę stosowaną w Disitool przez Didiera Stevensa, pobierając certyfikat cyfrowy podpisany przez Microsoft i importując go do złośliwego pliku wykonywalnego.

SET Menu

SET to oparty na menu system ataku, który jest dość unikalny, jeśli chodzi o narzędzia hakerów. Decyzja, aby nie wyświetlać go w wierszu poleceń, została podjęta z powodu tego, jak zdarzają się ataki socjotechniczne; wymaga wielu scenariuszy, opcji i dostosowań. Gdyby narzędzie było oparte na linii poleceń, naprawdę ograniczyłoby skuteczność ataków i niemożność pełnego dostosowania go do twojego celu.



Attack Vectors

- **(Spear-Phishing Attack Vector)** Wektor ataku typu spear-phishing może służyć do wysyłania ukierunkowanych wiadomości e-mail ze złośliwymi załącznikami, który może być wysyłany do wielu osób lub do pojedynczych, integruje się z pocztą Google i można go całkowicie dostosować do potrzeb użytkownika. Ogólnie jest to bardzo skuteczne w przypadku e-maili typu phishing spear.
- **(Java Applet Attack Vector)** Aplet Java jest jednym z głównych wektorów ataków w ramach SET. Atak Java Applet spowoduje utworzenie złośliwego Java Applet, który po uruchomieniu całkowicie zaszkodzi ofierze. Ciekawą sztuczką z SET jest to, że możemy całkowicie sklonować stronę internetową, a gdy ofiara kliknie „Uruchom", przekieruje ona ofiarę z powrotem do oryginalnej strony, dzięki czemu atak będzie bardziej wiarygodny. W tym wektorze ataku można wybrać szablony stron internetowych, które są zdefiniowanymi stronami, które zostały już zebrane, lub zaimportować własną.

- **(Metasploit Browser Exploit Method)** Metoda wykorzystująca przeglądarkę Metasploit zaimportuje exploity po stronie klienta Metasploit z możliwością klonowania witryny i wykorzystania exploitów opartych na przeglądarce.
- **(Credential Harvester Attack Method)** Metodę ataku modułu gromadzącego dane uwierzytelniające stosuje się, gdy nie chcemy konkretnie uzyskać powłoki, ale przeprowadzamy ataki phishingowe w celu uzyskania nazwy użytkownika i hasła z systemu. W tym wektorze ataku strona internetowa zostanie sklonowana, a gdy ofiara wprowadzi poświadczenia użytkownika, nazwy użytkownika i hasła zostaną odesłane z powrotem na komputer, a następnie ofiara zostanie przekierowana z powrotem do legalnej witryny.
- **(Tabnabbing Attack Method)** Metodę ataku Tabnabbing stosuje się, gdy ofiara ma otwartych wiele kart, gdy użytkownik kliknie link, otrzyma komunikat „Czekaj, trwa ładowanie strony”. Gdy przełącza karty, ponieważ wykonuje wiele zadań, witryna wykrywa obecność innej karty i przepisuje stronę na podanej stronie.

- **(Man Left in the Middle Attack Method)** "The man left in the middle attack" korzysta z REFERERÓW HTTP na już zaatakowanej stronie lub wykorzystuje luki w XSS, aby przekazać referencje z powrotem do serwera HTTP. W tym przypadku, jeśli znajdziesz lukę w zabezpieczeniach XSS i wyślesz adres URL do ofiary, a ona kliknie, witryna będzie działać w 100 procentach, jednak po przejściu do logowania do systemu przekaże poświadczenia z powrotem osobie atakującej i zbierze poświadczenia.
- **(Web Jacking Attack Method)** Metoda Web Jacking Attack utworzy klon witryny i wyświetli ofierze link z informacją, że witryna została przeniesiona. Na przykład, jeśli nasz sklonowany gmail, adres URL po najechaniu na niego myszką powinien to być tym prawdziwym gmailem ofiary. Gdy użytkownik kliknie w przeniesiony link, gmail zostaje otwarty, a następnie jest szybko zastępowany przez złośliwy serwer WWW.

- **(Multi-Attack Web Vector)** Multi-attack web vector jest nowością w wersji 0.7.1 i umożliwia określenie wielu metod ataku sieciowego w celu przeprowadzenia pojedynczego ataku. Umożliwia włączanie i wyłączanie różnych wektorów oraz łączenie ataków w jedną konkretną stronę internetową. Tak więc, gdy użytkownik kliknie link, będzie celem każdego z określonych wektorów ataku. W oparciu o wektory ataku nie należy ich łączyć.
- **(Teensy USB HID Attack Vector)** Teensy USB HID Attack Vector to niezwykłe połączenie spersonalizowanego sprzętu i obejścia ograniczeń przez emulację klawiatury. Urządzenie oparte na Teensy HID można emulować klawiaturę i mysz. Po włożeniu urządzenia zostanie ono wykryte jako klawiatura, a dzięki mikroprocesorowi i wbudowanej pamięci flash możesz wysłać bardzo szybki zestaw naciśnięć klawiszy do urządzenia i całkowicie go skompromitować.

- **(SMS Spoofing Attack Vector)** Ten moduł pozwoli nam sfałszować swój numer telefonu i wysłać SMS. Byłoby to korzystne w atakach socjotechnicznych wykorzystujących Credential Harvester.
- **(Wireless Attack Vector)** SET ma wektor ataku zwany wektorem ataku bezprzewodowego, który odrodzi punkt dostępu z karty interfejsu bezprzewodowego na twoim komputerze i wykorzysta DNSSpoof do przekierowania żądań przeglądarki ofiary do wektora atakującego w SET.
- **(QRCode Attack Vector)** The QRCode attack vector wykorzystuje możliwość generowania kodów QR natywnie w Pythonie. Po zeskanowaniu przekieruje do wektora ataku SET. Wspaniałą cechą tego ataku jest możliwość przekierowywania ofiar do dowolnego z wbudowanych wektorów ataku, jakie ma dla nich SET.

KONIEC! Dziękujemy za uwagę!