Usługi socjotechniczne:

- Rekonesans
- Złośliwe e-maile
- Złośliwe telefony

Usługi socjotechniczne: Rekonesans

Rozpoznanie to początkowa faza ataków przeciwko organizacjom, wykorzystująca w większości dane dostępne z publicznych źródeł. W zależności od zaprojektowanego (dalszego) zestawu wektorów ataku ma na celu zidentyfikowanie źródeł wiedzy na temat organizacji pod względem:

- ogólnych informacjach na jej temat
- danych jej pracowników
- wewnętrznej struktury organizacyjnej
- minionych i aktualnych zdarzeń ważnych w kontekście organizacji
- danych technicznych na wszelkich poziomach

Jest wykonywana w obu trybach:

- pasywnym (bez ingerencji w środowisko celu)
- aktywnym (bazując na zaprojektowanych interakcjach z celem)

Podstawowym założeniem rozpoznania jest wykonanie szczegółowej analizy i syntezy danych dostępnych o organizacji w zewnętrznych źródłach w celu budowy ukierunkowanych wektorów ataku, możliwych do wykorzystania w ramach symulacji lub rozważań teoretycznych (np. w ramach analizy ryzyka).

Usługi socjotechniczne

Scenariusz A: e-mail zawierający link do złośliwej strony	Scenariusz B: e-mail zawierający złośliwy dokument	Scenariusz C: telefony do pracowników w celu wyłudzenia danych
Cel: Nakłonienie pracownika do odwiedzenia strony z formularzem i podanie danych logowania AD (nazwy użytkownika i hasła) Scenariusz zakłada wykonanie przez pracownika operacji otwarcia strony internetowej (ukrytej pod rzeczywistym adresem linka firmowego), w celu potwierdzenia zaprojektowanej akcji. Po przejściu na stronę, pracownik widzi formularz z danymi do logowania **Śledzone akcje, to:** ■ Otwarcie maila przez pracownika (jeśli ten udostępni obrazki w kliencie poczty email) ■ Kliknięcie na link w wiadomości email ■ Podanie danych dostępowych w formularzu. **Realizacja scenariusza:** ■ Zakup domeny, ■ Przygotowanie szablonu emaila, ■ Przygotowanie docelowej strony internetowej, ■ Wysłanie emaila testowego do Klienta, ■ Weryfikacja i akceptacja emaila przez Klienta, ■ Wysłanie emaila do pracowników przygotowanego adresu, ■ Wysłanie powtórnie emaila z przypomnieniem do pracowników, którzy nie otworzyli maila pierwotnego, ■ Podsumowanie wyników i prezentacja.	**Cel:** Przesłanie wiadomości email z załącznikiem zawierającym odnośnik do zewnętrznego zasobu zawierającego złośliwy kod. Nakłonienie pracownika do otworzenia załącznika w zakładanym programu. Scenariusz zakłada zaprojektowanie uzasadnienia przesłania pliku konkretnego formatu w mailu (CV, lista awansów, akcja promocyjna) do wybranych pracowników. W ramach dokumentu znajdować się ma załącznik zawierający odpowiednio zdefiniowane akcje (pobranie danych, uruchomienie skryptu itp.. **Śledzone akcje, to:** ■ Otwarcie maila przez pracownika (jeśli ten udostępni obrazki w kliencie poczty email) ■ Pobranie złośliwych danych z poziomu zakładanego oprogramowania ■ (opcjonalnie) wykonanie dalszych akcji na systemie operacyjnym Klienta **Realizacja scenariusza:** ■ Zakup domeny, ■ Przygotowanie dokumentów w zakładanym formacie zaciągających złośliwą zawartość z zewnętrznej strony/ usługi, ■ Przygotowanie szablonu wiadomości email, ■ Wysłanie wiadomości email testowego do Klienta, ■ Weryfikacja i akceptacja wiadomości email przez Klienta, ■ Wysłanie wiadomości email do pracowników z przygotowanego adresu ■ Wysłanie powtórnie wiadomości email z przypomnieniem do pracowników, którzy nie otworzyli maila pierwotnego ■ Podsumowanie wyników i prezentacja	**Cel:** Nakłonienie pracowników przez telefon do wykonania zaprojektowanej akcji. Scenariusz wykonywany jest przez połączenie telefoniczne, w ramach którego pracownik zostanie nakłoniony na bazie zaprojektowanej historii do przekazania danych lub wykonania akcji. **Realizacja scenariusza:** ■ Zakup dodatkowych numerów telefonów ■ Zaprojektowanie schematu rozmowy oraz grafu możliwych odpowiedzi ■ Wstępne omówienie scenariusza ■ Wykonanie telefonów do pracowników ■ Powtórne wykonanie telefonów do pracowników, którzy nie odebrali telefonu ■ Podsumowanie wyników