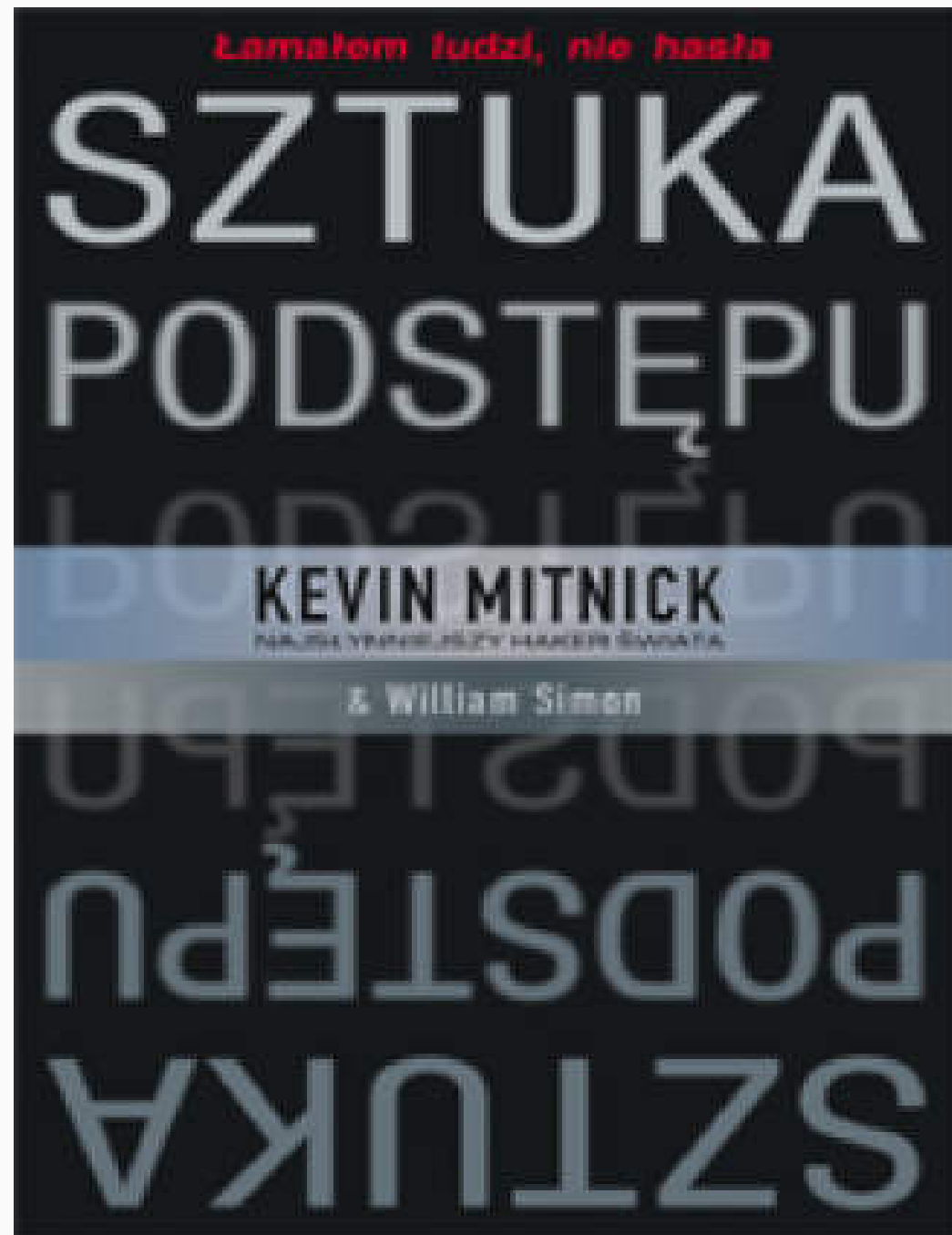


“Łamałem ludzi a nie hasła” -
czy Kevin Mitnick mógłby dziś
działać tak samo jak w latach
światności?





Kevin Mitnick, William L. Simon



Kevin David Mitnick, ps. Condor
“Najlepszy hacker świata”

(Współ)Autor książek:

- Sztuka podstępu
- Sztuka infiltracji
- Duch w sieci

Źródło: https://pl.wikipedia.org/wiki/Kevin_Mitnick

Socjotechnika

Zestaw manipulacyjnych technik psychologicznych i behawioralnych, polegających na wykorzystaniu błędów, słabości oraz naturalnych mechanizmów zaufania w celu nakłonienia osoby do wykonania określonego działania

Phreaking

Charakterystyka	Opis prezentacyjny
Definicja	Eksploracja, eksperymentowanie i manipulowanie systemami telekomunikacyjnymi, zwłaszcza w celu wykonywania darmowych połączeń lub uzyskiwania kontroli nad liniami.
Mechanizm Działania	Phreakerzy, w tym Mitnick, używali urządzeń generujących specjalne tony (np. <i>blue boxy</i> generujące ton 2600 Hz), aby oszukać systemy central telefonicznych i uzyskać dostęp do trybu operatora. Pozwalało to na: wykonywanie darmowych połączeń dalekodystansowych oraz zdobywanie dostępu do wewnętrznych systemów komunikacyjnych firmy, co było wstępem do inżynierii społecznej.
Znaczenie dla Mitnicka	Zrozumienie, jak działają sieci i systemy telefoniczne, było jego „szkołą hakerstwa”. Dało mu dostęp do narzędzi i wiedzy potrzebnej do późniejszego, większego <i>social engineeringu</i> (np. dzwonienie na koszt firmy).

Inżynieria Społeczna (Social Engineering)

Charakterystyka	Charakterystyka
Definicja	Sztuka manipulowania ludźmi w celu wykonania przez nich określonych czynności lub ujawnienia poufnych informacji.
Mechanizm działania	Mitnick bazował na naturalnej chęci ludzi do bycia pomocnym oraz na ich skłonności do ulegania autorytetom. Tworzył wiarygodne <i>preteksty</i> i wykorzystywał <i>kryzysowe</i> sytuacje, by skłonić ofiary do ujawnienia haseł, numerów kont lub szczegółów dotyczących infrastruktury.
Przykłady Pretekstów	Podszywanie się pod technika IT: "Jestem z działu technicznego. Mamy awarię serwera. Potrzebuję Pana/Pani hasła, by zdiagnozować problem." Podszywanie się pod dostawcę/konsultanta: "Dzwonię z firmy [znanej w branży]. Muszę zweryfikować konfigurację sieci przed jutrzejszą instalacją sprzętu."
Kluczowy Cel	Ominięcie zabezpieczeń technicznych poprzez bezpośrednie atakowanie najsłabszego ogniwa – człowieka.

Włamania do Systemów Komputerowych

Charakterystyka	Opis prezentacyjny
Definicja	Nieautoryzowany dostęp do zdalnych sieci, serwerów i stacji roboczych poprzez wykorzystanie luk w zabezpieczeniach systemów operacyjnych i protokołów sieciowych.
Mechanizm Działania	Mitnick używał m.in. techniki IP Spoofing (fałszowania adresu IP, aby system uznał, że żądanie pochodzi z zaufanego komputera w sieci) oraz wykorzystywał luki w popularnych protokołach TCP/IP (np. ataki oparte na sekwencji numerów).
Słynne Cele	Włamania do systemów firm takich jak Sun Microsystems, Novell, Motorola, IBM – celem było pozyskanie poufnego kodu źródłowego, autorskiego oprogramowania lub danych klientów.
Kluczowy Wniosek	Mitnick pokazał, że wiedza o architekturze systemu i protokołach w połączeniu z social engineeringiem jest zabójczą mieszanką. Używał socjotechniki, aby uzyskać szczegóły o konfiguracji systemu, a następnie używał wiedzy technicznej do włamania.

Techniki Fizycznej Inwigilacji i Podszywania się

Charakterystyka	Opis prezentacyjny
Definicja	Wykorzystanie fizycznej bliskości do celu w celu pozyskania informacji lub nieautoryzowanego dostępu do chronionych stref.
Mechanizm Działania	Tailgating (Piggybacking): Podążanie tuż za autoryzowanym pracownikiem przez drzwi o kontrolowanym dostępie. Udawanie, że zapomniało się karty dostępu lub trzymanie teczki/kartonów, aby osoba otwierająca drzwi czuła się zobowiązana do ich przytrzymania. Dumpster Diving: Przeszukiwanie śmietników w poszukiwaniu wyrzuconych dokumentów (haseł, numerów telefonów, harmonogramów, list wewnętrznych pracowników).
Znaczenie	Te techniki były kluczowe, ponieważ dostarczały wiarygodnych danych początkowych (np. imion, stanowisk, numerów wewnętrznych), które Mitnick następnie wykorzystywał w <i>pretextingu</i> telefonicznym, uwiarygadniając swoje fałszywe tożsamości.



Dziękuję :)

smaga.krzysztof@gmail.com

#CyberDlaOpornych