Testy Penetracyjne

Testy zabezpieczeń fizycznych i socjotechnika

Arkadiusz Chrobot

Katedra Systemów Informatycznych

8 maja 2024

Plan

Wstęp

Fizyczny dostęp do systemów i infrastruktury sieciowej zwykle jest gwarantowany w przypadku prowadzenia testów metodą znanego lub częściowo znanego środowiska. Pozwala on ocenić zabezpieczenia z innej perspektywy, niż w przypadku dostępu zewnętrznego. W przypadku testów prowadzonych metodą nieznanego środowiska mogą pojawić się wymagania dotyczące sprawdzenia zabezpieczeń fizycznych otoczenia np. centrów danych. Jest to działalność wykraczająca poza zagadnienia ściśle informatyczne, zatem zlecana jest stosunkowo rzadko, jednak osoby profesjonalnie zajmujące się testami penetracyjnymi powinny znać to zadnienie. Inną metodą weryfikacji stosowaną w testach penetracyjnych, której stosowanie nie jest często zlecane, a czasami wprost zabraniane, jest socjotechnika (ang. *social engineering*). Okazuje się, że jest to jednak bardzo skuteczna technika uzyskiwania nieuprawnionego dostępu, dlatego warto zasugerować zleceniodawcą sprawdzenie jej skuteczności w jego firmie/organizacji.

Zabezpieczenia fizyczne

Cel stosowania *zabezpieczeń fizycznych* ma pięć składowych [1]:

zniechęcenie—wykrycie—zaalarmowanie—opóźnienie—reakcję

Zniechęcenie jest osiągane wyglądem chronionego zasobu, który może prezentować się jako dobrze strzeżony lub niezwracający uwagi. Przeciwdziała przypadkowym intruzom, „korzystającym z okazji". Wykrycie dokonywane jest przez czujniki, których zadaniem jest powstrzymywanie intruzów działających z rozmysłem. Alarmy mają zwracać uwagę personelu odpowiedzialnego za bezpieczeństwo fizyczne, a bariery opóźniać działania osoby je naruszającej [2]. Są one również elementem reakcji.

Zabezpieczenia fizyczne

Testowanie fizycznych zabezpieczeń, podobnie jak testowanie systemów informatycznych wymaga wcześniejszego rekonesansu. Jednakże w tym przypadku musi on być wykonany w inny sposób [3]. Polega on na obserwacji celu testów, w poszukiwaniu słabych punktów i istotnych informacji, takich jak rutyny personelu ochraniającego, lista pracowników, wygląd identyfikatorów, zewnętrzne firmy mające dostęp do chronionych budynków, itd. Przeprowadzenie czynności zwiadowczych może wymagać ich dokumentowania, np. przy pomocy kamery, analizy zdjęć, w tym satelitarnych, a nawet przeszukiwania śmieci (ang. *dumpster diving*).

Zabezpieczenia fizyczne

Chronione pomieszczenia

Dostęp do pomieszczeń chronionych można czasem uzyskać bez używania wyrafinowanych środków technicznych. W niektórych przypadka wystarcza wykorzystanie socjotechniki, polegającej np. na podaniu się za kuriera dostarczającego przesyłkę, lub pracownika zakładu elektrycznego, który musi przeprowadzić inspekcję instalacji. Istotny jest zatem *pretekst* oraz odpowiednie rekwizyty (ubiór, narzędzia, itp.). Fałszywy identyfikator też może stanowić przepustkę gwarantującą wejście na strzeżony teren. Jeżeli wejście do budynku wymaga otwarcia drzwi przy użyciu specjalnego klucza, to można wykorzystać metodę polegającą na wejściu tuż za uprawnionym pracownikiem (ang. *tailgating, piggybacking*).

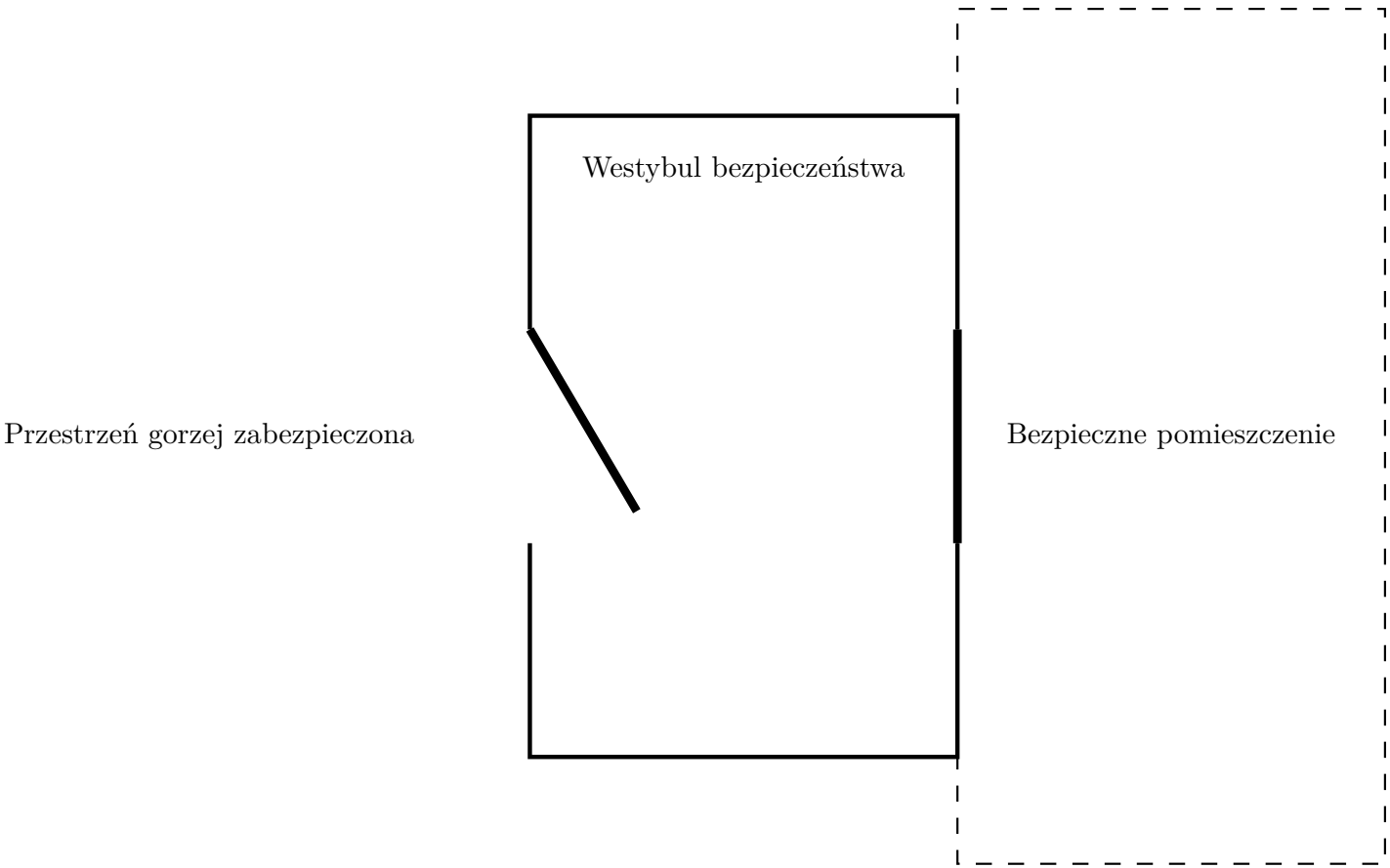
Zabezpieczenia fizyczne

Chronione pomieszczenia

Takim sytuacjom zapobiega, przedstawiony schematycznie na Rysunku 1, *westybul bezpieczeństwa* (ang. *security vestibule*). Jest to pomieszczenie podobne do śluzy, w którym może przebywać w danym momencie tylko jedna osoba. Dodatkowo, drzwi prowadzone do chronionego pomieszczenia mogą być otwarte tylko wtedy, gdy te prowadzące do przestrzeni gorzej chronionej są zamknięte.

Zabezpieczenia fizyczne

Chronione pomieszczenia



Rysunek: Projekt typowego westybulu bezpieczeństwa

Zabezpieczenia fizyczne

Ogrodzenia i monitoring

Wykonując testy zabezpieczeń fizycznych warto zwrócić uwagę na ogrodzenia, które stanowią bariery mające na celu odgrodzenie terenu chronionego od niezabezpieczonego. Mogą one mieć różną formę, od żywopłotu lub słupków zabezpieczających przez przypadkowym wtargnięciem, po betonowe, wzmocnione mury, osadzone głęboko w gruncie, aby uniemożliwić wykonanie podkopu i zabezpieczone drutem kolczastym lub żyletkowym, by utrudnić pokonanie ich górom. Istnieje kilka standardów, w tym przygotowanych przez NIST, określających gdzie i jakie ogrodzenia powinny być stosowane. Jednak nawet rozbudowane rozwiązania mogą posiadać słabe punkty. W szczególności należy upewnić się, że nie można obejść ogrodzenia, np. korzystając z dachów sąsiadujących budynków. Jeśli jest zainstalowany na ogrodzeniu lub w jego pobliżu monitoring, to trzeba sprawdzić, czy nie ma w nim martwych stref, tzn. obszarów nie obejmowanych przez kamery.

Zabezpieczenia fizyczne

Zamki

Wejście do pomieszczeń może wymagać sforsowania prowadzących do niego drzwi. Wbrew obiegowym opiniom zamek nie jest ▸ pierwszym celem dla większości intruzów. Najczęściej słabym punktem są zawiasy, które można uszkodzić i umożliwić tym samym dosłownie „wyjęcie” lub „wypchnięcie” drzwi. Takiemu zagrożeniu mogą przeciwdziałać specjalne śruby do mocowania zawiasów. Inny problem mogą stanowić drewniane ościeżnice, które mogą być „rozepchnięte” przy pomocy np. hydraulicznych drążków rozporowych i dać taki sam rezultat, jak uszkodzone zawiasy. Szczeliny między skrzydłami drzwi lub ościeżnicą mogą umożliwić wykorzystanie drutu lub innego materiału do cofnięcia rygla lub dźwigni antypanicznej. Jeśli od wewnątrz jest zainstalowany detektor wyjścia (ang. *egress sensor*) reagujący na podczerwień, to można go oszukać sprężonym powietrzem. W przypadku sensorów reagujących na ludzką sylwetkę możliwe są inne ▸ rozwiązania.

Zabezpieczenia fizyczne

Zamki

Jeśli jedyną opcją pozostaje forsowanie zamka w drzwiach, to dalsze działania zależą od jego rodzaju. Większość zamków mechanicznych jest podatna na metodę uderzeniową (*bumping*), która jednak wymaga posiadania specjalnego klucza i może prowadzić do całkowitego uszkodzenia urządzenia. Innym rozwiązaniem jest skorzystanie z wytrychów. W Stanach Zjednoczonych powstała nawet legalna organizacja o nazwie TOOOL, która prowadzi w tym zakresie szkolenia. Należy jednak pamiętać, że w Polsce, zgodnie z artykułem 129 Kodeksu Wykroczeń (slajd nr 12), legalnie posiadać mogą wytrychy ślusarze, oraz osoby, które uzyskały policyjną licencję pracownika zabezpieczenia technicznego (źródło: https://serwis-zamkow.com/posiadanie-narzedzi-do-otwierania-zamkow-oraz-ich-legalnosc/).

Zabezpieczenia fizyczne

Zamki

Art. 129 **KW** (źródło: https://lexlege.pl/kw/art-129/)

§1. Kto:

1) wyrabia, posiada lub nabywa wytrychy, jeżeli nie trudni się zawodem, w którym są one potrzebne,
2) dostarcza wytrychów osobie nietrudniącej się takim zawodem,
3) wyrabia, posiada lub nabywa klucze do cudzego domu, mieszkania lub innego pomieszczenia albo schowania bez zezwolenia osoby uprawnionej lub organu administracji,

podlega karze aresztu, ograniczenia wolności albo grzywny.

§2. Tej samej karze podlega, kto wyrabia, posiada lub nabywa narzędzia przeznaczone do dokonywania kradzieży albo kto dostarcza takich narzędzi innym osobom.

§3. Wytrychy, klucze lub narzędzia podlegają przepadkowi, choćby nie stanowiły własności sprawcy.

Zabezpieczenia fizyczne

Zamki

Zamki elektroniczne niekoniecznie mogą stanowić większe wyzwanie niż zamki mechaniczne. Kod do tych, które wyposażone są w klawiaturę numeryczną można podejrzeć obserwując, bezpośrednio lub za pośrednictwem kamer lub innych urządzeń, wchodzących do pomieszczenia pracowników. Jeśli zamek jest otwierany kartą RFID, to może ona zostać sklonowana. Niekiedy wystarczy w tym celu urządzenie ▸ Flipper Zero, które zostało zaprezentowane na Rysunku 2. Na rynku dostępne są trzy rodzaje kart RFID:

- niskiej częstotliwości (125–134,2 kHz);
- wysokiej częstotliwości (13,56 MHz), nazywane także kartami (NFC);
- ultra wysokiej częstotliwości (865–928 MHz).

Im wyższy zakres częstotliwości pracy karty, tym trudniej ją sklonować, choć w przypadku kart NFC taką możliwość mogą oferować smartfony.

Zabezpieczenia fizyczne

Zamki

Rysunek: Flipper Zero (źródło: https://en.m.wikipedia.org/wiki/File:Flipper_Zero.jpg)

Zabezpieczenia fizyczne

Zamki

W przypadku kart NFC można zastosować atak przekazania (ang. *relay attack*), która wymaga dwóch osób. Pierwsza przy pomocy czytnika z nadajnikiem odczytuje kartę, która nie znajduje się w pobliżu zamka. Druga, wyposażona w odbiornik, odbiera sygnał i przekazuje go do zamka. Z kolei dla zamków ze zmiennym kodem, uruchamianych np. pilotem można zastosować atak odtworzenia (ang. *replay attack*), do którego można np. użyć radia HackRF One, wspomnianego na poprzednim wykładzie. W tym wypadku atak polega na nasłuchiwaniu sygnału z pilota i jednoczesnym blokowaniu odbiornika. W momencie, gdy pojawi się drugi sygnał z pilota, to należy go zarejestrować, a przepuścić do odbiornika przechwycony wcześniej pierwszy. W ten sposób uzyskuje się „zapasowy" sygnał, który można wykorzystać później.

Zabezpieczenia fizyczne

Zamki

Zamki biometryczne również nie stanowią doskonałego zabezpieczenia. Większość metod rozpoznawania biometrycznego bazuje na statystyce, co powoduje, że przy dużej liczbie zarejestrowanych użytkowników rośnie prawdopodobieństwo, że będą „myliły" niektóre osoby. W przypadku biometrii najlepsze rezultaty dają systemy oparte na skanowaniu siatkówki. Jednakże nawet one mają problemy z ludźmi o ciemnych kolorach oczu lub z naturalnie powiększonymi źrenicami. Dodatkowo niektóre nie są odporne na ataki wykonane przy pomocy zdjęć oczu w dużej rozdzielczości.

Zabezpieczenia fizyczne

Alarmy

Alarmy mogą zostać zneutralizowane przy użyciu różnych środków technicznych, ale warto zwrócić uwagę, że ich skuteczność jest powiązania z tym jak na nie reaguje personel odpowiedzialny za ochronę obiektu. Może to wykorzystać intruz wszczynając fałszywe alarmy, które w końcu uśpią czujność strażników.

Zabezpieczenia fizyczne

Czujniki

Istnieje kilka rodzajów czujników stosowanych jako zabezpieczenia fizyczne:

- sensory wibracji,
- przełączniki w drzwiach i oknach,
- pasywne czujniki na podczerwień,
- detektory ruchu działające w oparciu o ultradźwięki lub mikrofale,
- bariery na podczerwień lub mikrofale,
- czujniki nacisku,
- kamery,
- czujniki przemieszczenia.

Każdy z nich może być w jakiś sposób sabotowany, np. przez odłączenie zasilania, zwarcie lub podmianę. Czujniki ruchu mogą nie wykrywać powolnego przemieszczania.

Socjotechnika

Socjotechnika (ang. *social engineering*) polega na wykorzystaniu ludzi, zamiast sytemu informatycznych, do pozyskania interesujących informacji [4]. Wymaga ona dobrego zrozumienia psychologi ludzkiej i tzw. miękkich umiejętności. Bazuje ona na wykorzystaniu następujących zjawisk:

zaufanie większość ludzi chce komuś ufać;

odwzajemnieniu ludzie są skłonni ulegać osobom, wobec których czują zobowiązanie;

autorytet ludzie słuchają osób, które mają nad nimi pozorną lub faktyczną władzę;

pośpiech zmuszą ludzi do bezrefleksyjnego działania;

strach działa podobnie jak pośpiech;

podobieństwo ludzie często ufają innym, w podobnej sytuacji;

dowód społeczny ludzie często naśladują innych;

niedobór ludzie chętnie zdobywają dobra unikatowe;

pomocna natura ludzie z natury bywają pomocni.

Socjotechnika

Technika bezpośrednia

Socjotechnika może wymagać bezpośredniego kontaktu testera z osobą będącą celem tej metody. Kontakt ten może przybrać różne formy:

zbieranie informacji na pozór swobodna rozmowa, której celem jest pozyskanie informacji;

wywiad/przesłuchanie udawana formalna rozmowa, np. o pracę;

qui pro quo zaoferowanie czegoś wartościowego, aby osoba docelowa poczuła się zobowiązana;

podglądanie przez ramię (ang. *shoulder surfing*) bliskie obserwowanie osoby, np. by poznać jej hasło do systemu;

atak typu USB Drop podrzucenie np. pamięci USB (pendrajw) z zainstalowanym złośliwym oprogramowaniem.

Niektóre podręczniki do testów wspominają również o przekupieniu, jednak w Polsce, z uwagi na regulacje prawne, ta metoda może mieć poważne konsekwencje (artykuł 228 i 229) i nie wolno jej stosować.

Socjotechnika

Phishing

Phishing pozwala intruzowi pozyskać ważne informacje najczęściej przy pomocy spreparowanej wiadomości e-mail. Istnieje jednak kilka typów tego ataku:

Vishing Polega na użyciu połączenia telefonicznego, zamiast wiadomości e-mail. Warto zauważyć, że bardzo łatwo jest podszyć się pod numer telefoniczny innej osoby, gdyż usługa *Caller*ID nie stosuje uwierzytelnienia.

SMS phishing Zamiast wiadomości e-mail wykorzystywane są SMSy.

Whaling To phishing skierowany wobec osób piastujących ważne stanowiska.

Spear phishing To phishing skierowany wobec jednej, konkretnej osoby.

Socjotechnika

Atak z użyciem stron WWW

W socjotechnice można wykorzystać także strony WWW i aplikacje internetowe. Najpopularniejsze tego typu ataki to:

Watering Holes Umieszczenie na stronie, często odwiedzanej przez osoby będące celem socjotechniki, złośliwego oprogramowania, które zainfekuje ich urządzenia.

Clonned Websites Sklonowanie prawdziwej strony, która jest wykorzystywana przez osobę będącą celem ataku. Klon tej strony niekoniecznie musi oferować te same funkcje, co oryginał, ale będzie np. rejestrował dane uwierzytelniające stosowane na prawdziwej stronie.

Socjotechnika

Narzędzia

Do popularnych narzędzi wspomagających stosowanie socjotechniki należą SET (ang. Social Engineering Toolkit) i BeEF (Browser Exploitation Framework). Pierwsze pozwala między innymi przygotować zainfekowany nośnik dla ataków typu USB Drop, wygenerować QR kod ze złośliwą zawartością lub stworzyć fałszywy punkt dostępowy do sieci Wi-Fi. Z kolei BeEF tworzy i udostępnia stronę WWW. Jeśli z tą stroną połączy się przeglądarka WWW, to to narzędzie pozwala uzyskać o niej informacje (ang. *fingerprinting*) i przejąć kontrolę na jej zachowaniem.

Literatura

Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. URL: https://www.cl.cam.ac.uk/~rja14/book.html.

Pete Herzog i ISECOM. *The Open Source Security Testing Methodology Manual*. 2010. URL: https://www.isecom.org/OSSTMM.3.pdf.

The Penetration Testing Execution Standard. 2014. URL: http://www.pentest-standard.org/index.php/Pre-engagement#Physical_Penetration_Test.

Security Through Education. 2024. URL: https://www.social-engineer.org.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!