BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 24, 2007

Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych

Adam E. PATKOWSKI

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Artykuł przestawia sformalizowaną metodykę prowadzenia testów penetracyjnych systemów teleinformatycznych. Metodyka P-PEN może zostać wykorzystana w samodzielnych przedsięwzięciach testów penetracyjnych, może też zostać użyta w ramach szerszych przedsięwzięć, w szczególności w audytach bezpieczeństwa teleinformatycznego prowadzonych zgodnie z opublikowaną w 2003 r. metodyką LP-A.

SŁOWA KLUCZOWE: bezpieczeństwo informacji, badania bezpieczeństwa, test penetracyjny, audyt, podatności

Niniejszy artykuł opisuje metodykę P-PEN wykonywania testów penetracyjnych – przedsięwzięcia zmierzającego do zidentyfikowania podatności („słabych punktów") w badanych systemach teleinformatycznych, prowadzonego ze znacznym udziałem eksperymentów.

Na wstępie warto zauważyć, że minimalistyczne rozumienie pojęcia „testy penetracyjne" to postępowanie „dokładnie jak hacker". Ortodoksi będą wręcz uważali, że w punkcie startowym testów nie powinna być dostępna nawet minimalna wiedza o atakowanym obiekcie, a wszystkie działania powinny odbywać się ogólną metodą „black box". To podejście ma swoje zalety: jest ciekawym wyzwaniem intelektualnym, świetną zabawą, powinno być wysoko płatne, także fascynujące – jeśli zrobi się z tego widowisko, ale użytecznych informacji daje niewiele. Co więcej, nie odpowiada nawet deklarowanemu modelowi postępowania „jak hacker".

Z drugiej strony, w wysoce użytecznych publikacjach, uznawanych za podstawowe i jednocześnie odpowiadające obecnemu stanowi technologii (np. [2], [3], [6], [8] lub [9]), widoczna jest tendencja do opatrywania nazwą „testy penetracyjne" przedsięwzięć w istocie stanowiących ocenę bezpieczeństwa teleinformatycznego, pod warunkiem, że owa ocena będzie zawierała dostatecznie obszerny udział badań technicznych.

Jak się wydaje, takie szerokie użycie nazwy „testów penetracyjnych" w miejsce znacznie właściwszego „audytu" lub „badania bezpieczeństwa teleinformatycznego" jest to naturalna reakcja środowiska inżynierów na napływ na rynek usług oceny bezpieczeństwa bezrobotnych ostatnio audytorów jakości, bez kwalifikacji technicznych, co owocuje „papierowymi audytami" oferowanymi pod nazwą „audyt bezpieczeństwa" właśnie. Papierowe audyty są dobrze przyjmowane przez menedżerów, bo zapewniają tanio ładne certyfikaty, wynik jest zwykle zgodny z pożądanym, a zalecenia pokontrolne nie wymagają zakupów drogiego sprzętu, tylko co najwyżej wytworzenia zaskakująco zrozumiałych dla menedżerów dokumentów. Poza tym raporty pisane są zrozumiałym językiem, a nie wpędzającym w kompleksy slangiem inżynierów. Nazwa „testy penetracyjne" jednoznacznie sygnalizuje wyrafinowane badania techniczne i raczej nie zostanie przejęta jako nazwa „papierowej" usługi.

Dalej testy penetracyjne rozważane są jako jeden ze sposobów zbierania informacji w ramach badania odporności/podatności (lub szerzej – bezpieczeństwa) systemów komputerowych.

Cechy wyróżniające testy penetracyjne spośród innych rodzajów poszukiwania podatności to:

- potwierdzanie zidentyfikowanych podatności przez precyzyjne wskazanie (często poparte pokazem) skutecznych ataków owe podatności wykorzystujących,
- tradycyjna przewaga technik heurystycznych, opartych zwykle na osobistym doświadczeniu realizujących badania ekspertów,
- ukrywanie tych sposobów przez firmy i ekspertów – wynikające z traktowania ich jako „know-how" nie podlegającego ochronie prawnej.

Dodać należy, że istotną konsekwencją tych cech jest wymaganie wysokich kwalifikacji wykonawców. Testy penetracyjne są postrzegane nawet w środowisku specjalistów jako zajęcie bliższe sztuce niż rzemiosłu. Dla zleceniodawcy oznacza to niestety całkowity brak kontroli nad tym, co właściwie zrobi wykonawca testów penetracyjnych, a także, co znacznie gorsze, brak informacji zarówno o wnikliwości, jak i skuteczności badań.

W miarę rozwoju dziedzin rozpoznawania podatności, rozpoznawane coraz nowe sposoby okazywały się niezbyt skomplikowane. Zauważono, że można zrezygnować ze wskazywania dokładnych sposobów wykorzystania podatności – wystarczało stwierdzić pojedyncze objawy lub przesłanki

występowania podatności i na tej podstawie wnioskować o obecności podatności i konieczności przeprowadzenia zabiegów naprawczych. Na rynku pojawiły się programy poddające przeglądowi różne atrybuty systemów komputerowych i w rezultacie raportujące występujące w owych systemach podatności. Takie programy to różnego rodzaju skanery – bezpieczeństwa, konfiguracji, zainstalowanego oprogramowania, portów itp. nazwano automatycznymi narzędziami rozpoznawana podatności. Obecnie można zauważyć, że przedstawiciele firm zajmujących się testami penetracyjnymi zwykle zaliczają badania za pomocą automatycznych narzędzi do podstawowych testów penetracyjnych – czasem nawet są to jedyne oferowane badania.

W 2003 roku opublikowano metodykę LP-A prowadzenia audytu bezpieczeństwa teleinformatycznego, która spotkała się z przychylnym przyjęciem środowiska specjalistów zajmujących się bezpieczeństwem informacji. Jedną z cech wyróżniających tej metodyki jest znaczny nacisk położony na tzw. „ścieżkę techniczną" badań, obejmujące także testy penetracyjne, rozumiane dość wąsko jako badania możliwości wykorzystania podatności prowadzone wyłącznie metodami heurystycznymi. W metodyce tej jako jeden z procesów ujęto „uzupełniające testy penetracyjne". Słowo „uzupełniające" wynika tu z poprzedzania testów penetracyjnych, wyłączonych jako samodzielny proces, obowiązkowymi badaniami prowadzonymi za pomocą skanerów, wyrywkowymi badaniami konfiguracji oraz badaniami zabezpieczeń fizycznych i technicznych.

Opisana w niniejszym opracowaniu metodyka P-PEN może zostać wykorzystana w samodzielnych przedsięwzięciach testów penetracyjnych, może też zostać użyta w ramach szerszych przedsięwzięć, w szczególności stanowić uzupełnienie LP-A w prowadzonych zgodnie z tą metodyką przedsięwzięciach audytu bezpieczeństwa teleinformatycznego.

Metodyka P-PEN została sformułowana dla osiągnięcia następujących celów:

- minimalizacji szans pominięcia którejkolwiek ze znanych podatności,
- pozostawienia ekspertom swobody w działaniu przy jednoczesnym ujęciu ich działania w możliwie ścisłe formalne ramy,
- uzupełnienia (wcześniej opublikowanej) metodyki LP-A audytu bezpieczeństwa teleinformatycznego o możliwie sformalizowany opis procesu prowadzenia testów penetracyjnych.

Główna idea metodyki P-PEN polega na przeprowadzeniu prac w trzech etapach: analizy, właściwych badań i syntezy (dalej nazywanej integracją wyników).

Etap analizy rozpoczyna się po dobraniu ekipy specjalistów o kwalifikacjach odpowiednich do elementów składowych systemu, w tym i jego zabezpieczeń. W początkowej fazie przedsięwzięcia mają oni za zadanie

opisać możliwe scenariusze ataków na zasoby badanego obiektu (zwykle systemu teleinformatycznego). Rozsądnym sposobem formułowania zbioru tych ataków jest organizacja moderowanej sesji, w której przeglądany jest pewien zadany zbiór kategorii ataków (por. Rozdział 7). W praktyce okazuje się, że eksperci traktują ten zbiór „kategorii" raczej jako zbiór haseł, nie zmienia to jednak faktu, że zmuszeni do zastanowienia i wypowiedzi na każde z nich, dokonują zupełnego przeglądu zagrożeń i sposobów ich szkodliwego wykorzystania. Należy podkreślić, że w ramach przeglądu eksperci mają za zadanie dla każdego hasła ocenić możliwość skojarzenia z nim jakiegoś złożonego (kombinowanego) ataku, prowadzącego do konkretnego celu. Inaczej mówiąc muszą oni sformułować opisy takich ataków kombinowanych, które prowadzą do atrakcyjnego z punktu widzenia napastnika lub szkodliwego z punktu widzenia zleceniodawcy, celu. Zbiór takich opisanych ataków nazwano „listą rozważanych ataków kombinowanych". Należy podkreślić, że eksperci w trakcie tej fazy działania mają okazję do wykazania się swą sztuką i pomysłowością. Jedynym ograniczeniem ich inwencji jest konieczność rozważania każdej z pozycji zadanego wstępnie zbioru ujętego metodyce w oddzielnym rozdziale (Rozdział 7 „Kategorie ataków"). Ten rozdział został sformułowany na podstawie własnych doświadczeń, gdyż zawartość żadnej z uznanych fundamentalnych publikacji, traktujących o metodach prowadzenia badań technicznych bezpieczeństwa (zwykle pod nazwą testów penetracyjnych: [2], [6], [8] oraz [9]), nie okazała się użyteczna w praktyce jako wzorzec zbioru kategorii ataków. Obiecująca klasyfikacja CAPEC ([1]) nie była analizowana. Wykaz kategorii ataków ujęty w metodyce nie jest zamknięty, nie jest też klasyfikacją ani nawet podziałem (różne pozycje można uznać za podstawę do wywiedzenia takich samych ataków kombinowanych). Ma on jednak niebagatelną zaletę – sprawdza się w praktyce zespołów ekspertów o bardzo różnym składzie. Wykaz ten wymaga również przed użyciem przeglądu i ściągnięcia najnowszych tzw. exploitów ze wskazanych miejsc ich publikacji w Internecie.

W dalszej części analizy, po sformułowaniu wykazu możliwych ataków, postępowanie jest już rutynowe: każdy z opisanych ataków kombinowanych zostaje rozpisany na poszczególne elementarne techniki składowe (wraz z miejscem i czasem użycia w ataku), po czym dla każdej techniki należy zapisać, jaki objaw lub przesłanka rozpoznawana w badanym systemie wskazuje na możliwe powodzenie tej techniki. „Objawem" może być zarówno pewien zapis konfiguracyjny, jak i pozytywny wynik pewnego wskazanego testu-ataku. Tak powstaje spis objawów i miejsc ich występowania, który kończy fazę analizy.

Należy zwrócić uwagę na jeszcze jeden spodziewany, ważny krok w etapie analizy: określenie pewnych fragmentów badanego obiektu (systemu teleinformatycznego), które odpowiadają zakresom stosowania poszczególnych

kategorii ataków. W praktyce okazuje się, że dla ekspertów, dokonujących przeglądu kategorii ataków po zapoznaniu się z systemem zleceniodawcy (obiektem badań), określanie takich fragmentów, do których stosuje się każda z kolejnych kategorii, nie stanowi problemu. Moderator sesji przeglądu kategorii ataków (jeśli taka jest wykonywana) powinien tylko zadbać o to, aby pytanie „czy jest jeszcze jakiś fragment systemu, dla którego rozpatrywana kategoria mogłaby być skuteczna?" pojawiało się systematycznie.

Drugą fazą w metodyce są właściwe testy: sprawdzenie, czy każdy z ujętych w spisie objawów w systemie występuje, czy też nie. Na postawie takiego „spisu objawów i miejsc ich występowania" z etapu analizy można wygenerować rozsądny plan testów penetracyjnych, grupując takie pozycje spisu, które mogą zostać sprawdzone przez pojedynczy zespół prowadzący badania z jednego miejsca w jednej dziedzinie.

Po przeprowadzeniu badań możliwe jest dla każdej pozycji spisu – techniki ataku – określenie szans na powodzenie i wskazania dla poprawy rozpoznanego stanu, należy jednak podkreślić, że jeśli takie dokumenty są oczekiwane, to przedsięwzięcie, w ramach którego prowadzone są testy penetracyjne, nie jest regularnym audytem. W ramach prezentowanej metodyki nie przewiduje się badań „black box", natomiast dla pełnego obrazu zagrożeń przeprowadza się także badania osiągalności informacji na temat atakowanego obiektu.

Ostatnim etapem metodyki jest etap syntezy. W wyniku etapu badania otrzymuje się informacje o skuteczności elementarnych technik ataków. Odwracając postępowanie z analizy, można zatem rozstrzygnąć, czy każdy ze sformułowanych na początku ataków kombinowanych będzie skuteczny, czy też nie. Końcowy raport jest prostą konsekwencją wnioskowania o zagrożeniach dla zasobów zleceniodawcy rozważanymi atakami. Raport daje zleceniodawcy obraz stanu zabezpieczeń jego sieci i systemów, co zwykle stanowi podstawę do dalszych działań w zakresie zabezpieczeń. Dodatkowo formułuje się dokładne scenariusze (także i „czarne scenariusze") rozpoznanych skutecznych ataków. Zwykle będą to po prostu uszczegółowione scenariusze sformułowane już bardziej ogólnie na etapie analizy, a prowadzące do sukcesu w badanym systemie.

Na koniec można przeprowadzić demonstrację skutecznych ataków, co jednak trudno uznać za działanie profesjonalne – pozytywne efekty da tylko jako działanie z zakresu kształtowania świadomości, co jest efektywne wyłącznie w zakresie podnoszenia odporności na ataki socjotechniczne i to tylko w środowiskach o wysokich kwalifikacjach informatycznych. W innych środowiskach taki eksperyment demonstracyjny pozostanie kompletnie niezrozumiany, a sprowokuje pewien typ pracowników do niebezpiecznych zabaw w hackerów.

W ramach metodyki P-PEN nie uwzględnia się explicite systematycznych badań kodu źródłowego oprogramowania badanego systemu ani wnikliwych inspekcji jego kodów binarnych (modułów ładowalnych). Na specjalne życzenie zleceniodawcy, przy okazji testów penetracyjnych możliwe jest prowadzenie poszukiwań objawów „incydentu w toku" lub śladów wcześniejszych przestępstw. Zawsze w przypadku wykrycia szczególnie groźnych podatności następuje przekazanie zleceniodawcy przez wykonawców wykazu podatności „do natychmiastowego usunięcia".

Metodykę P-PEN sformułowano w ten sposób, aby mogła ona zostać wykorzystana zarówno jako jeden z procesów metodyki LP-A, jak i jako metodyka prowadzenia samodzielnego przedsięwzięcia. W przypadku prowadzenia testów penetracyjnych jako samodzielnego przedsięwzięcia, formalnie rzecz biorąc badania zabezpieczeń F-T oraz badania zautomatyzowanymi narzędziami prowadzone są równolegle z badaniami prowadzonymi technikami leżącymi w dziedzinie teleinformatyki („właściwymi" testami penetracyjnymi).

Podobnie jak w przypadku metodyki LP-A, tak i dla P-PEN na podstawie informacji zamieszczonych w opisie metodyki można ocenić złożoność procesów metodyki, rozpoznać zależności pomiędzy wytwarzanymi dokumentami, dobrać skład zespołu wykonawczego oraz ułożyć plan przedsięwzięcia, przewidując jego czas trwania i koszty. Nie bez znaczenia może być też fakt, że w przypadku znajomości metodyk, zarówno LP-A, jak i P-PEN przez obie zainteresowane strony (zleceniodawcę i zleceniobiorcę), posługują się one jednolicie rozumianą terminologią i posiadają jednolitą podstawę pojęciową do prowadzenia dyskusji i podejmowania konkretnych decyzji.

Jako załącznik artykułu przedstawiono metodykę P-PEN w formie oddzielnego, zamkniętego dokumentu, stanowiącego jej formalny zapis. Na pewien niedostatek elegancji formalnej cierpi rozdział 7 („Kategorie ataków"). Jest on jednak sformułowany do wykorzystania w praktyce jako wzorzec zbioru kategorii ataków, a nie jako wyczerpująca klasyfikacja na jakimś ustalonym poziomie ogólności. Stąd otwarta postać listy, w której w każdym punkcie zawarto pozycję (…) oznaczającą „inne".

Literatura

[1] CAPEC *Common Attack Pattern Enumeration and Classification, Classification Tree*, http://capec.mitre.org (stan na koniec 2007 r.).

[2] *Information Systems Security Assessment Framework (ISSAF), Draft 0.2.1B*. http://www.oissg.org, OISSG 2006.

[3] Kenneth R. van Wyk: *Penetration Testing Tools*, Carnegie Mellon University, 2007.

[4] Liderman K., Patkowski A.E.:. *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, Biuletyn IAiR Nr 19, WAT, Warszawa, 2003.

[5] *OWASP testing guide 2007 V2.0*, OWASP Foundation, 2007.

[6] Pete Herzog: *OSSTMM 2.2. Open-Source Security Testing Methodology Manual*. http://www.isecom.org, ISECOM, 2006.

[7] Sean Barnum, Amit Sethi: *Attack Pattern Usage*, https://buildsecurityin.us-cert.gov Cigital, Inc., 2006

[8] T. J. Klevinsky, Scott Laliberte, Ajay Gupta: *Hack I.T.: Security Through Penetration Testing*. Addison Wesley, 2002.

[9] Tiller J.S.: *The Ethical Hack. A Framework for Business Value Penetration Testing*. Auerbach Publications (CRC Press LLC), Washington, 2005.

The P-PEN penetration testing methodology

ABSTRACT: The article presents the formal methodology of penetration security testing of TI systems. P-PEN methodology may be used in independent undertakings of testing and it may also be used in much broader undertakings, mainly in security audits performed according to LP-A methodology (published in 2003).

KEYWORDS: information security, security testing, penetration testing, audit, vulnerability

Recenzent: prof. dr hab. inż. Włodzimierz Kwiatkowski

Praca wpłynęła do redakcji: 19.06.2007 r.

ZAŁĄCZNIK

Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych

Spis treści

Wykaz używanych terminów i symboli graficznych 71
Wstęp 74
Rozdział 1. Skład zespołu, kwalifikacje jego członków i zakresy kompetencji 77
Rozdział 2. Wyposażenie narzędziowe zespołu 78
Szablony edycyjne dokumentów 79
Aktualny zbiór exploitów 81
Skanery portów 81
Skanery bezpieczeństwa 81
Skanery konfiguracji 81
Rozdział 3. Procesy 82
Rozdział 4. Specyfikacja dokumentów 84
Tabele IPO 84
Specyfikacja zbiorcza dokumentów 87
Rozdział 5. Diagramy przepływu danych 89
Rozdział 6. Rzetelne praktyki 89
Rozdział 7. Kategorie ataków 93

Wykaz używanych terminów i symboli graficznych

TERMINY

Atak – celowe, intencjonalne działanie przeciw cudzym interesom. [Atak nie musi być nielegalny. Przedmiotem ataku może być obiekt nie należący do ofiary, nie leżący w obszarze jej administracji, ale jeśli napastnik oddziaływa na niego z intencją zaszkodzenia ofierze osiągając ten cel, to jest to skuteczny atak przeciw ofierze.]

Obiekt ataku – element systemu informatycznego: zasób, urządzenie, łącze, użytkownik lub operator, na którym dokonywane są zabiegi prowadzące do celu ataku.

Ofiara ataku – podmiot: osoba fizyczna lub prawna, której interesy zostają narażone na szwank w wyniku ataku.

Cel ataku – ostateczne zmiany stanu fizycznego, prawnego lub informacji, do których osiągnięcia zmierza napastnik, zwykle powodujące straty dla ofiary ataku.

Źródło ataku – miejsce, z którego prowadzone są działania napastnika. W atakach teleinformatycznych jest nim zwykle komputer napastnika. Termin ten staje się niejednoznaczny w przypadku ataków za pomocą automatycznych lub zdalnie sterowanych narzędzi ataku.

Atak na system teleinformatyczny i informację w nim przetwarzaną – nieuprawnione, celowe działania ludzi mające na celu naruszenie tajności, integralności lub dostępności informacji.

Atak kombinowany – złożone działanie, w którym napastnik wykorzystuje więcej niż jedną z elementarnych technik (sposobów) działania przeciw atakowanemu obiektowi. Co więcej, atak kombinowany składa się zwykle z szeregu działań elementarnych, z których część może zostać zakwalifikowana jako elementarne ataki pośrednie, wymierzone przeciw innym obiektom niż atak kombinowany, a zatem przynoszące szkody innym podmiotom niż ofiara ataku kombinowanego. Część działań składowych może być neutralna, a nawet pozytywna w skutkach, a zatem nie kwalifikować się jako ataki.

Audyt – postępowanie dla oceny zgodności audytowanego obiektu z wzorcem (normą, wzorcem proceduralnym lub arbitralnie ustanowionym wektorem wartości pewnych cech) prowadzone przez stronę niezależną (firmę, osobę lub zespół). W przypadku audytu z zakresu bezpieczeństwa teleinformatycznego, ta niezależność powinna być zachowana w stosunku do:

1) organizacji/zespołu budującego system zabezpieczeń;
2) dostawców sprzętu i oprogramowania;
3) organizacji podlegającej przeglądowi w takim sensie, że w skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt.

Audytor – członek zespołu audytowego przeprowadzający badania i analizy.

Audytor kwalifikujący – członek zespołu audytowego uprawniony do formułowania ocen uogólniających z badań przeprowadzonych przez zespół audytowy; w szczególności uprawniony do ferowania ostatecznych sądów audytowych o zgodności rozpoznanego stanu rzeczy z generalnym wzorcem audytowym.

Bezpieczeństwo – stopień racjonalnie uzasadnionego (np. analizą ryzyka) zaufania, że potencjalne straty nie zostaną poniesione, (pot.) – niepodleganie obawie; spokój; pewność, że się nic złego nie stanie.

Bezpieczeństwo teleinformatyczne – stopień uzasadnionego zaufania (por. np. ISO/IEC 15408) że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za

pomocą systemów teleinformatycznych nie zostaną poniesione.

Exploit – rutynowy algorytm (często w postaci skryptu lub programu) wykorzystania podatności systemu komputerowego na szkodę jego bezpieczeństwa.

Incydent w toku – atak w trakcie trwania. Dotyczy nie tylko czasu ingerencji hackera w system, ale np. całego czasu pozostawania automatycznego szpiega w systemie.

Informacja wrażliwa – dla określonego podmiotu są to wszelkie informacje, które mogą zostać wykorzystane przeciwko temu podmiotowi poprzez ujawnienie, uniedostępnienie oraz zmanipulowanie jawne lub skryte. W szczególności, są to wszystkie informacje, które muszą być chronione, bo tak nakazują obowiązujące przepisy prawne (np. ustawa „*o ochronie danych osobowych”*) oraz takie informacje, których nakaz ochrony nie jest zawarty w żadnych regulacjach prawnych, a które dla konkretnych organizacji je wytwarzających i przetwarzających, są wskazywane przez kompetentne organy, np. służby ochrony państwa, wewnętrzne komórki bezpieczeństwa w danej organizacji, pełnomocnika ds. bezpieczeństwa informacji itp.

Kategoria ataku – grupa ataków, scharakteryzowana pewną charakterystyczną wspólną cechą; wśród ekspertów zwykle panuje zgoda co wyróżnienia takich grup (chociaż częściej używa się określenia „typ ataku”). Określenie kategorii ataków (i szczególnych jej reprezentantów) powinno być dokonane na podstawie aktualnego stanu wiedzy,

Metodyka (gr. *methodikós* 'metodyczny' od *méthodos* 'badanie; metoda') 1. zbiór zasad, sposobów wykonywania określonej pracy a. osiągnięcia określonego celu; 2. szczegółowe normy postępowania właściwe danej nauce. (Władysław Kopaliński „*Słownik wyrazów obcych i zwrotów obcojęzycznych*” Wyd. De Agostini Polska).

Obiekt badań – poddawany badaniu obiekt, tu: system, program lub zbiór danych, którego cechy szczególne: atrybuty, sposób zachowania się, podlegają rozpoznaniu w trakcie badań.

Ochrona fizyczna – zapewnianie bezpieczeństwa za pomocą personelu, zwykle wyspecjalizowanego: strażników, patroli interwencyjnych itd. wyposażonego w odpowiednie środki techniczne i przymusu bezpośredniego, w razie potrzeby uzbrojonego.

Przedmiot badań – rozpoznawane w trakcie badań wielkości, atrybuty, cechy zachowania się obiektu badań.

Podatność (ang. *vulnerability*) – wady lub luki struktury fizycznej, organizacji, procedur, personelu, zarządzania, administrowania, sprzętu lub oprogramowania, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika.

UWAGI

1 – Istnienie podatności nie powoduje szkód samo z siebie. Podatność jest jedynie warunkiem lub zestawem warunków, które umożliwiają uszkodzenie systemu lub zakłócenie działalności użytkownika przez atak

2 – jeśli podatność odpowiada zagrożeniu, istnieje ryzyko.

(*punkt 3.1.064 w PN-I-02000:1998*)

Środki bezpieczeństwa – środki fizyczne (np. płot), techniczne (np. system alarmowy), ludzkie (np. wartownik), programowe (np. oprogramowanie antywirusowe) lub działania organizacyjne (np. szkolenia), stosowane w celu przeciwdziałania wykorzystaniu podatności przez zagrożenia. Często, w skrócie, środki bezpieczeństwa są nazywane **zabezpieczeniami.**

Test „black box” – test penetracyjny prowadzony bez wiedzy na temat badanego obiektu przekazanej jawnie przez zleceniodawcę.

Test penetracyjny – badanie: eksperyment (również prezentacyjny) służący weryfikacji hipotezy o podatności badanego obiektu lub jego w pełni adekwatnego odpowiednika.

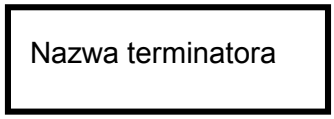
Zabezpieczenia techniczne – polegające na (wg *Ustawy o ochronie osób i mienia*): montażu elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia, oraz montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach zainstalowania.

Zagrożenie (ang. *threat*) – potencjalne naruszenie zabezpieczeń systemu informatycznego
(*punkt 3.1.115 w PN-I-02000:1998*)

Zasoby teleinformatyczne – wszelkie zasoby fizyczne (np. sejf), techniczne (np. urządzenia klimatyzacyjne, komputery), informacyjne w różnej postaci (np. papierowa dokumentacja techniczna sieci, zawartość elektronicznych baz danych) do których nieupoważniony dostęp lub zniszczenie może być przyczyną utraty poufności, integralności lub dostępności informacji przetwarzanych, przechowywanych i przesyłanych w systemach i sieciach teleinformatycznych.

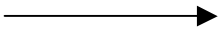
SYMBOLE GRAFICZNE

symbol **procesu** na DFD



symbol **terminatora**, tj. elementu zewnętrznego w stosunku do procesów opisywanych za pomocą DFD.

symbol **magazynu**, tj. elementu mogącego gromadzić dane (dokumenty lub inne, zależne od modelowanego kontekstu, elementy).



symbol **przepływu** danych (dokumentów, informacji itd.) pomiędzy elementami DFD.

UWAGA
Symbole graficzne procesów i magazynów, rysowane na diagramach DFD linią przerywaną, oznaczają procesy i magazyny opcjonalne – występujące w przypadku realizacji testów penetracyjnych jako samodzielnego przedsięwzięcia, nie występujące natomiast w przypadku realizacji testów penetracyjnych jako elementu audytu prowadzonego zgodnie z (wcześniej opublikowaną) metodyką LP-A przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego.

Wstęp

Niniejszy dokument opisuje metodykę P-PEN wykonywania testów penetracyjnych – przedsięwzięcia badań technicznych zmierzającego do zidentyfikowania podatności („słabych punktów") w badanych systemach teleinformatycznych prowadzonego ze znacznym udziałem eksperymentów.

W 2003 roku opublikowano metodykę LP-A prowadzenia audytu bezpieczeństwa teleinformatycznego, która spotkała się z przychylnym przyjęciem środowiska specjalistów zajmujących się bezpieczeństwem informacji. Jedną z cech wyróżniających tej metodyki jest znaczny nacisk położony na tzw. „ścieżkę techniczną" badań, obejmującą także testy penetracyjne. W metodyce LP-A jako proces o numerze 4.3.6 ujęto „uzupełniające testy penetracyjne". Słowo „uzupełniające" wynika tu z poprzedzania testów penetracyjnych, wyłączonymi jako samodzielne procesy, badaniami prowadzonymi narzędziami automatycznymi (4.3.2 i 4.3.3), badaniami konfiguracji (4.3.1) oraz badaniami zabezpieczeń fizycznych i technicznych (F-T, proces 4.2). Jak łatwo stąd wywnioskować, testy penetracyjne definiowane są na potrzeby LP-A dość wąsko jako badania możliwości identyfikacji najnowszych lub bardzo wyrafinowanych podatności (np. na złożone ataki kombinowane) prowadzone metodami heurystycznymi.

Na przedstawioną dalej metodykę P-PEN prowadzenia testów penetracyjnych składają się:

1) organizacja, zakresy kompetencji i kwalifikacje zespołu (rozdział 1)
2) wyposażenie narzędziowe zespołu (rozdział 2)
3) dokumenty niezbędne do zainicjowania przedsięwzięcia oraz wytwarzane w jego trakcie (rozdział 4)
4) model w postaci diagramów DFD opisujący procesy wytwarzania dokumentów i powiązania pomiędzy nimi (rozdział 3 oraz rozdział 5)
5) wykaz tzw. „rzetelnych praktyk", tj. heurystycznych sposobów postępowania, wypracowanych i sprawdzonych podczas dotychczasowej praktyki (rozdział 6).

Do przedstawienia procesów i przepływu dokumentów, zostały wykorzystane elementy metody strukturalnej projektowania systemów informatycznych. Elementy te, to przede wszystkim tabele IPO (ang. *Input-Process-Output*), diagramy przepływu danych (DFD – ang. *Data Flow Diagram*) oraz stosowane na nich oznaczenia procesów, przepływów i magazynów (por. „*Wykaz używanych terminów i symboli graficznych*" na początku niniejszego opracowania).

Metodykę P-PEN sformułowano w ten sposób, aby mogła zostać wykorzystana zarówno jako proces 4.3.6 metodyki LP-A (por. rozdział 3 dalej)**, jak i jako metodyka prowadzenia samodzielnego przedsięwzięcia testów penetracyjnych.** Ponieważ w tym drugim przypadku zakres metodyki jest nieco szerszy, w opisach (zarówno w tabelach IPO, jak i diagramach DFD) elementy wykraczające poza LP-A oznaczono liniami przerywanymi.

Metodyka P-PEN została sformułowana dla osiągnięcia następujących celów:

- pozostawienia ekspertom swobody w działaniu przy jednoczesnym ujęciu ich działania w ścisłe formalne ramy;
- opisania postępowania w ramach przedsięwzięcia testów penetracyjnych w stopniu możliwie sformalizowanym;
- zapewnienia pełnego udokumentowania postępowania wykonawców w trakcie prowadzenia testów;

- ograniczenia do minimum możliwości nie rozpoznania znanych podatności (znanych według stanu wiedzy z ustalonego dnia, zwykle początkowego dnia przedsięwzięcia) dzięki usystematyzowaniu, czy wręcz zrutynizowaniu działań zespołu wykonawców;
- uzupełnienia (wcześniej opublikowanej) metodyki LP-A audytu bezpieczeństwa teleinformatycznego o możliwie sformalizowany opis prowadzenia testów penetracyjnych.

Główna idea metodyki P-PEN polega na przeprowadzeniu prac w trzech etapach: analizy, właściwych badań i syntezy (dalej nazywanej integracją wyników).

A. Analiza

Maksymalne zrutynizowanie polega na pozostawieniu pełnej swobody specjalistom z dziedziny ataków informacyjnych tylko w jednym punkcie postępowania: gdy w początkowej fazie przedsięwzięcia mają oni za zadanie opisać możliwe scenariusze ataków na zasoby badanego obiektu (zwykle systemu teleinformatycznego). Sposób formułowania zbioru takich ataków jest jednak sterowany: powinien on powstać drogą przeglądu pewnego zadanego zbiór kategorii ataków (na przykład takiego, jak prezentuje rozdział 7). Dla każdej z tych kategorii należy sformułować opisy takich ataków, które prowadzą do pewnych atrakcyjnych z punktu widzenia potencjalnych napastników, lub szkodliwych z punktu widzenia Zleceniodawcy, celów. Opisywane ataki powinny zawierać techniki ataków należące do rozpatrywanej kategorii. Zbiór takich opisanych ataków nazwano „listą rozważanych ataków kombinowanych".

Od tej pory, zgodnie z metodyką P-PEN, postępowanie jest już rutynowe: każdy z opisanych ataków kombinowanych zostaje rozpisany na poszczególne elementarne techniki (indywidualizowane m.in. urządzeniami lub podsystemami, przeciw którym są skierowane), po czym dla każdej techniki należy zapisać jaki jest objaw/przesłanka wskazująca na to, że zastosowanie owej techniki w tym konkretnym miejscu zostanie uwieńczone powodzeniem. „Objawem" może być zarówno pewien zapis konfiguracyjny, jak i pozytywny wynik pewnego wskazanego testu-ataku. Taki spis objawów i spodziewanych miejsc ich występowania kończy fazę analizy.

B. Właściwe badania

Na postawie takiego spisu z etapu analizy można wygenerować plan testów penetracyjnych, grupując takie pozycje spisu, które mogą zostać sprawdzone przez pojedynczy zespół prowadzący badania z jednego miejsca w jednej dziedzinie. Po przeprowadzeniu badań możliwe jest dla każdej pozycji spisu – techniki ataku – określenie, czy określone dla niej objawy/przesłanki są spełnione.

Jeśli przedsięwzięcie, w ramach którego prowadzone są testy penetracyjne nie jest regularnym audytem, możliwe jest sformułowanie wskazań (tzw. „rekomendacji") dla poprawy rozpoznanego stanu.

C. Synteza

W wyniku badania otrzymuje się informacje o spodziewanej skuteczności elementarnych technik ataków. Odwracając postępowanie z analizy, można zatem rozstrzygnąć, czy każdy ze sformułowanych na początku ataków kombinowanych będzie skuteczny, czy też nie. Końcowy raport jest prostą konsekwencją wnioskowania o zagrożeniach dla zasobów Zleceniodawcy rozważanymi atakami. Dodatkowo w raporcie można ująć dokładne scenariusze (także i tzw. „czarne scenariusze") rozpoznanych skutecznych ataków.

W przypadku prowadzenia testów penetracyjnych jako samodzielnego przedsięwzięcia, formalnie rzecz biorąc badania zabezpieczeń fizycznych i technicznych (F-T) oraz badania zautomatyzowanymi narzędziami prowadzone są równolegle z badaniami („właściwymi" testami penetracyjnymi) prowadzonymi technikami leżącymi w dziedzinie teleinformatyki.

Metodyka P-PEN zachowuje główne cechy z metodyki LP-A, cyt.: „Cechą charakterystyczną metodyki LP-A jest, w ramach tzw. *ścieżki technicznej*, realizacja badań systemów ochrony fizycznej i technicznej oraz sieci i systemów teleinformatycznych eksploatowanych w badanym obiekcie. **Badania te są przeprowadzane przy użyciu wyspecjalizowanych narzędzi i są uzupełniane testami penetracyjnymi**, głównie heurystycznymi.

Efektem przyjęcia takiego schematu postępowania jest:

1) możliwość wykrycia szczególnie groźnych podatności i przekazanie Zleceniodawcy przez audytorów wykazu podatności „do natychmiastowego usunięcia" (odrębną kwestią pozostaje, kto ma usuwać zidentyfikowane podatności – ze względów formalnych nie powinien tego robić zespół prowadzący testy);
2) przekazanie Zleceniodawcy pełnego obrazu (zarówno technicznego jak i organizacyjnego) stanu zabezpieczeń jego sieci i systemów, co zwykle stanowi podstawę do dalszych działań Zleceniodawcy w zakresie bezpieczeństwa teleinformatycznego."

Podobnie jak w przypadku metodyki LP-A, tak i dla P-PEN na podstawie informacji zamieszczonych w opisie metodyki można:

1) ocenić złożoność procesów metodyki;
2) rozpoznać zależności pomiędzy wytwarzanymi dokumentami;
3) dobrać skład Zespołu, uwzględniając wymagane zakresy kompetencji (kwalifikacji i uprawnień) jego członków;
4) ocenić na podstawie zależności pomiędzy procesami (oraz składu osobowego Zespołu) możliwości równoległego prowadzenia poszczególnych działań;
5) ułożyć harmonogram prac;
6) oszacować koszty przeprowadzenia prac.

Rozdział 6 prezentuje tzw. „rzetelne praktyki" (nazywane też „najlepszymi praktykami" – z ang. *best practices*) tj. należące do kategorii know-how metody lub zasady postępowania, wypracowane i sprawdzone podczas dotychczasowej praktyki. Chociaż praktyki takie zostały wymienione wcześniej jako element metodyki, to należy zauważyć, że są one ściśle związane z konkretnym zespołem ludzi (ich kwalifikacjami, doświadczeniem, etyką itd.). Z tego względu zawartość rozdział 6 należy traktować jako wskazówkę – każdy zespół prawdopodobnie wypracuje sobie własny zestaw „rzetelnych praktyk".

W konstrukcji metodyki zmierzano do rozdzielenia części podlegającej silnej formalizacji – opisującej postępowanie i dokumentowanie według ustalonych reguł, od części słabo sformalizowanej, dotyczącej swobodnego poszukiwania rozwiązań (ataków). W opisie ową część słabo poddającą się formalizacji wyłączono w oddzielny rozdział 7 („Kategorie ataków") zawierający informacje, dla których przewiduje się najkrótszy czas aktualności. Stanowi on wykaz obszarów, w których należy szukać skutecznych ataków na badany system. Ten rozdział został sformułowany na podstawie doświadczeń, gdyż zawartość żadnej z uznanych fundamentalnych publikacji, traktujących o metodach prowadzenia badań technicznych bezpieczeństwa (zwykle pod nazwą testów penetracyjnych: [2], [3], [6], [8] oraz [9]) nie okazała się użyteczna jako wzorzec zbioru kategorii ataków. Wykaz kategorii ataków powinien podlegać stałej aktualizacji w miarę zmian stanu sztuki.

Rozdział 1. Skład zespołu, kwalifikacje jego członków i zakresy kompetencji

W tym rozdziale są przedstawione informacje na temat składu i kwalifikacji zespołu. Sposób pracy, wynikający z praktycznie wdrożonej i sprawdzonej metodyki zawiera rozdział 3. Zespół wykonawców składa się z dwóch części: stałej i zmiennej („na telefon"). Dalej opisano role członków zespołu – role te mogą być łączone. Wyróżniono zalecane role dwóch członków zespołu odpowiadających za całość przedsięwzięcia, dla których to ról, dla zgodności z metodyką LP-A, zachowano nazwę „audytorzy kwalifikujący",

I. Skład stały zespołu

1. **Audytorzy kwalifikujący** – dwie osoby (symbole: AK_1 i AK_2)
   Wymagania:
   a) wykształcenie wyższe techniczne
   b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie badań systemów komputerowych, w szczególności w zakresie bezpieczeństwa teleinformatycznego
   c) co najmniej kilkuletnia praktyka w przeprowadzaniu audytów/przedsięwzięć z zakresu bezpieczeństwa teleinformatycznego
   d) doświadczenie dydaktyczne oraz umiejętność prowadzenia negocjacji
   e) dopuszczenia odpowiednich krajowych władz bezpieczeństwa do dostępu do informacji niejawnych (np. w Polsce, w rozumieniu ustawy „*o ochronie informacji niejawnych*").

   Do podstawowych zadań audytorów kwalifikujących należy:
   – wykonanie przedsięwzięć z etapu przygotowawczego (jeśli testy penetracyjne są samodzielnym przedsięwzięciem – por. rozdział 3)
   – uzgodnienie planu testów i zasad podziału odpowiedzialności
   – nadzór nad wykonywaniem badań
   – przekazanie stronie Zleceniodawcy wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia"
   – opracowanie dokumentu końcowego.

   Audytorzy kwalifikujący podpisują się pod dokumentami końcowymi jako gwaranci rzetelności zawartych w nich informacji.

2. **Specjalista od urządzeń sieciowych i sieci komputerowych** (symbol: SUS-SK)
   Wymagania:
   a) wykształcenie wyższe techniczne
   b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych oraz w zakresie organizacji i obsługi sieci oraz budowy urządzeń sieciowych
   c) praktyka w przeprowadzaniu badań i/lub audytów z zakresu bezpieczeństwa teleinformatycznego
   d) dopuszczenia odpowiednich Krajowych Władz Bezpieczeństwa do dostępu do informacji niejawnych (np. w Polsce, w rozumieniu ustawy „*o ochronie informacji niejawnych*").

   Do zadań specjalisty od urządzeń sieciowych i sieci komputerowych należy:
   – wskazanie ekspertów dziedzinowych (na etapie przygotowania umowy)
   – opracowanie planu testów (proces 3)
   – nadzór nad pracami ekspertów dziedzinowych (por. rozdział 3)
   – współudział w opracowaniu raportów.

3. **Personel pomocniczy** (symbol: PP)
   Personel pomocniczy, zajmujący się np. kopiowaniem, oprawianiem itp. stosownych dokumentów musi posiadać dopuszczenia odpowiednich Krajowych Władz Bezpieczeństwa do dostępu do informacji niejawnych (np. w Polsce, w rozumieniu ustawy „*o ochronie informacji niejawnych*") w przypadku prac z takimi dokumentami. W szczególnych przypadkach (np. ankieterzy), personel taki musi posiadać odpowiednie upoważnienia Zleceniodawcy do przeprowadzenia określonych prac na terenie jego Instytucji.

II. Skład zmienny zespołu (symbol: ED)
Skład zmienny zespołu stanowią dobierani w miarę potrzeb eksperci dziedzinowi. Eksperci dziedzinowi są dobierani przez audytorów kwalifikujących według wskazań specjalisty - sieciowca dla potrzeb konkretnego przedsięwzięcia, w zależności od systemów (sprzętu i oprogramowania) szczególnie licznych lub szczególnie ważnych w badanym systemie komputerowym (np. Solaris, Windows XP, Novell, itd.) oraz konkretnych wymagań osobowych dotyczących np. posiadania dopuszczeń do informacji niejawnych. Jeśli przedsięwzięcie obejmuje rozpoznanie zabezpieczeń fizycznych i technicznych, należy powołać specjalistę w tym zakresie:

4. ***Specjalista od ochrony fizycznej i technicznej*** *(symbol: SF-T)*
   Wymagania:
   a) wykształcenie wyższe
   b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych, w szczególności w zakresie bezpieczeństwa teleinformatycznego
   c) praktyka w przeprowadzaniu audytów z zakresu bezpieczeństwa teleinformatycznego
   d) licencja pracownika zabezpieczenia technicznego II stopnia
   e) dopuszczenia odpowiednich Krajowych Władz Bezpieczeństwa do dostępu do informacji niejawnych (np. w Polsce, w rozumieniu ustawy „o ochronie informacji niejawnych").
   Do zadań specjalisty od ochrony fizycznej i technicznej należy:
   – *realizacja procesu 5.3 (por. rozdział 3) w przypadku, gdy testy penetracyjne realizowane są jako samodzielne przedsięwzięcie;*
   – *udział w procesie integracji wyników (proces 6) – prezentacja wyników badań F-T na potrzeby skuteczności ataków.*

Rozdział 2. Wyposażenie narzędziowe zespołu

Do narzędzi, którymi dysponuje zespół należą: szablony edycyjne dokumentów, oraz aktualny zbiór tzw. exploitów (programów i skryptów pozwalających identyfikację i wykorzystanie podatności systemów). Do wyposażenia zespołu zaliczyć można też narzędzia zautomatyzowane (programy), głównie skanery portów, skanery bezpieczeństwa oraz skanery konfiguracji.

W przypadku audytu prowadzonego zgodnie z metodyką LP-A automatyczne narzędzia wykorzystywane są obligatoryjnie w odrębnych procesach (badaniach). W przypadku testów penetracyjnych prowadzonych jako samodzielne przedsięwzięcie

użyteczne wydaje się wykorzystanie automatycznych narzędzi po prostu dlatego, że ich raporty zawierają gotowe odpowiedzi na pytania o występowanie w systemie elementarnych objawów podatności na większość podstawowych technik ataków. Należy podkreślić, że raporty te są tylko częścią pomocniczego materiału badawczego, oszczędzającego planowania i ręcznego wykonywania podstawowych sprawdzeń i eksperymentów.

Szablony edycyjne dokumentów

Dla większości dokumentów wykorzystywanych w postępowaniu zgodnym z metodyką P-PEN wypracowano szablony dotyczące co najmniej ich redakcji, a w części przypadków ustalające rozmieszczenia merytorycznych treści. Zbiorczy wykaz dokumentów ujęto w tabeli 1. Niniejsze opracowanie nie zawiera szablonów edycyjnych dokumentów, ale dla najważniejszych z nich podano niżej główne oczekiwane elementy merytoryczne:

1. Wytyczne do testów penetracyjnych (por. „Wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych" w tab. 1):
   - 1.1. Identyfikacja obiektu badania (systemu teleinformatycznego) i precyzyjne określenie jego granic
   - 1.2. Wskazanie zasobów z oceną ich wrażliwości
   - 1.3. Określenie przedmiotu badania (dziedziny właściwości, parametrów oraz zachowania się obiektu podlegające badaniu dla identyfikacji występujących podatności)
   - 1.4. Ograniczenia dotyczące zakresu i obiektu badań (czasu, dopuszczalnych wyłączeń, jego dostępności dla badań, ewentualnej dostępności środowiska testowego lub adekwatnych makiet)
   - 1.5. Szczegółowe procedury uzgodnień działania (z przedstawicielami Zleceniodawcy)
2. „Lista rozważanych ataków kombinowanych"; dla każdej pozycji listy:
   - 2.1. Definicja sukcesu
   - 2.2. Oszacowanie strat w przypadku powodzenia
   - 2.3. Wykaz elementarnych działań (technik ataków i niezbędnych działań dopuszczalnych) i/lub cech elementów obiektu (konfiguracji badanego systemu) niezbędnych do powodzenia ataku
3. „Wykaz elementarnych ataków"; dla każdej pozycji:
   - 3.1. Numery macierzystych pozycji (ataków kombinowanych) z listy rozważanych ataków kombinowanych – dla których powodzenie elementarnego działania (ataku) jest warunkiem koniecznym skuteczności
   - 3.2. Istota działania (którego powodzenie jest niezbędne) lub własności konfiguracyjnej
   - 3.3. Definicja sukcesu
   - 3.4. Lista przesłanek lub objawów wystarczająca do wnioskowania o podatności któregoś z elementów obiektu na ten atak elementarny (wnioskowania o spodziewanym sukcesie ataku)
4. „Wyselekcjonowana lista ataków do badań ręcznych" – zbiorcza lista pozycji wg punktu 3.4 powyżej, podzielona według dziedzin (według pozycji 4.4 poniżej); dla każdej pozycji:
   - 4.1. Obiekt badania (urządzenie, zbiór konfiguracyjny, łącze, program, zabezpieczenie F-T, operator, strażnik itd.)
   - 4.2. Przesłanki na podstawie których wnioskowano o możliwej podatności obiektu
   - 4.3. Wskazanie narzędzia lub metody badania

4.4. Wskazanie dziedziny:
4.4.1. Teleinformatyczne (w tym łącza) i socjotechniczne: właściwe testy penetracyjne
4.4.2. Zabezpieczenia techniczne, ppoż. lub ochrona fizyczna
4.4.3. Zasilania (energetyczne, inne media, klimatyzacja)
4.4.4. Leżące w zakresie badań narzędziami automatycznymi w poszukiwaniu podatności
4.4.5. Leżące w zakresie badań narzędziami automatycznymi w poszukiwaniu błędów konfiguracji
4.4.6. Leżące w zakresie badań narzędziami automatycznymi w poszukiwaniu opóźnień w aktualizacjach

5. „Plan testów penetracyjnych i przeglądów konfiguracji"; lista zadań badawczych, dla każdego zadania składająca się z:
5.1. Wykazu wykonawców realizujących zadanie
5.2. Miejsca, w którym/z którego będą prowadzone badania (w tym adresy przestrzenne i sieciowe)
5.3. Podzbioru pozycji z wyselekcjonowanej listy ataków (punkt 4 powyżej) do zbadania
5.4. Harmonogram badania
5.5. Wynikające z badań obciążenie zasobów (w tym personelu) i usług Zleceniodawcy
5.6. Możliwe zagrożenia dla zasobów Zleceniodawcy i innych podmiotów
5.7. Procedury szczegółowe postępowania
5.7.1. Sposób nadzoru przez Zleceniodawcę (zgoda na rozpoczęcie, informacja o kolejnym kroku, odpowiedzi na pytania, informacja o zakończeniu)
5.7.2. Zasady stymulacji lub modyfikacji w systemie Zleceniodawcy wprowadzanych na potrzeby badania (np. wydłużenie czasu dzierżawy DHCP na czas wielodniowego skanowania lub zablokowanie tworzenia dynamicznych reguł na zaporach sieciowych z inicjatywy systemów IDS na czas badań, w szczególności skanerami bezpieczeństwa)
5.8. Zasady odpowiedzialności za skutki działań

6. Sprawozdanie z badania – autoryzowane, jeśli odbywało się pod nadzorem personelu Zleceniodawcy (por. „Notatki służbowe – sprawozdania z badań i przeglądów konfiguracji" w tab. 1).
6.1. Czas działania zespołu i lokalizacja każdego z miejsc, w którym/z którego odbywało się badanie
6.2. Wykaz czynności
6.3. Wyniki
6.3.1. W części formalnej: dokładny odpowiednik wyselekcjonowanej listy ataków, przy czym dla każdej zaplanowanej do badania pozycji określa się wynik (podatność: występuje,/nie występuje/badanie nie dostarczyło jednoznacznych wyników/badanie nie powiodło się/odstąpiono od wykonania badania)
6.3.2. W części opisowej: dodatkowe wyjaśnienia i obserwacje, szczególnie jeśli odstąpiono od badania
6.4. Informacja o współpracy z personelem Zleceniodawcy

7. Wykaz „Podatności do natychmiastowego usunięcia"
8. Raport z testów penetracyjnych – por. „Raport z testów penetracyjnych (wyniki ręcznych testów penetracyjnych)" w tab. 1
8.1. Sprawozdanie z działań

8.2. Ogólny wykaz podatności
8.3. Ustosunkowanie się do wszystkich pozycji z listy ataków kombinowanych
8.4. Scenariusze skutecznych ataków (w tym konieczna wiedza i środki napastnika)
8.5. Czarne scenariusze (przy założeniu, że wszystko sprzyja napastnikowi, niektóre środki ochrony zawodzą)
8.6. Oceny szans zajścia i powodzenia poszczególnych ataków i w konsekwencji ocena możliwych strat
8.7. Zintegrowana ocena zagrożenia

Aktualny zbiór exploitów

W badaniach wykorzystuje się również tzw. exploity oraz autentyczne narzędzia ataków, aktualizowane bezpośrednio przed rozpoczęciem testów penetracyjnych. Zwykle do tej klasy zalicza się również odpowiednie autorskie opracowania członków zespołu.

Skanery portów

Skanery portów to automatyczne narzędzia odwołujące się wybranych portów za pomocą spreparowanych pakietów i wspomagające wnioskowanie z odpowiedzi na te pakiety. Zwykle wykorzystywane jako narzędzie w „ręcznych" testach penetracyjnych.

Skanery bezpieczeństwa

Skaner bezpieczeństwa to program, lub sterowany tym programem system komputerowy, przeglądający komputery należące do pewnego zadanego zbioru i sprawdzający obecność w nich podatności. W modelu ogólnym, obiektem przeglądanym przez skaner bezpieczeństwa jest iloczyn kartezjański zbioru komputerów poddanych badaniu oraz zbioru podatności. Dla każdego elementu (podatności na komputerze) określana jest wartość funkcji obecności (podatność: występuje/nie występuje).

Wynikiem działania skanera bezpieczeństwa jest raport, który w swym podstawowym wydaniu zawiera dla każdego komputera wykaz zidentyfikowanych (występujących w nim) podatności, a dla każdej podatności określa: identyfikator według uznanej klasyfikacji (np. *bugtraq*), opis, stopień zagrożenia oraz sposób usunięcia.

Skaner bezpieczeństwa jest zbiorem procedur (czasem programów lub skryptów) przeprowadzających w praktyce próby ataków. Każdy zakończony powodzeniem atak jest odnotowywany i informacja o nim jest umieszczana w raporcie końcowym generowanym przez skaner.

Skanery bezpieczeństwa zawierają zbiory sygnatur podatności i wzorce ataków. Dane te powinny być aktualizowane w miarę zmian stanu sztuki w tej dziedzinie. Subskrypcja tych danych jest w ofercie producentów komercyjnych skanerów bezpieczeństwa.

Skanery konfiguracji

Formalnie rzecz biorąc skanery konfiguracji wykorzystywane będą podczas testów penetracyjnych prowadzonych jako samodzielne przedsięwzięcie. W przypadku audytu prowadzonego zgodnie z metodyką LP-A automatyczne narzędzia wykorzystywane są w odrębnych procesach.

Skaner konfiguracji to program służący do automatycznego, zdalnego badania ustawień konfiguracyjnych (w tym tzw. zasad zabezpieczeń) każdego z komputerów należących do wybranego zbioru, generujący odpowiednie raporty. Badanie polega na dostępie do plików konfiguracyjnych (np. do rejestru systemu MS Windows) badanego

komputera i porównaniu zawartych w tych plikach zapisów z wzorcem uznanym za właściwy przez producenta skanera. Skanery konfiguracji poddają również sprawdzeniu zapisy w plikach konfiguracyjnych dotyczące zainstalowanych poprawek (patches) dystrybuowanych przez producentów – braki takich poprawek sygnalizowane są jako podatności. Wadą skanerów konfiguracji jest konieczność zdalnego dostępu do badanych komputerów z uprawnieniami administratora, co jest naturalne w sieciach domenowych Windows, ale jest niezgodne z zasadami bezpieczeństwa w większości sieci o innej organizacji.

Rozdział 3. Procesy

W dalszej części tego rozdziału opisano ogólnie, z komentarzami, procesy, oraz podano (tabela 1) kto z Zespołu odpowiada za każdy proces i kto go nadzoruje.

W przypadku, gdy przedsięwzięcie testów penetracyjnych jest realizowane jako składowe audytu bezpieczeństwa teleinformatycznego prowadzonego zgodnie z metodyką LP-A, odpowiada ono jednemu z procesów tej metodyki:

4.3.6. Wykonanie uzupełniających testów penetracyjnych.

Może także objąć kolejny proces:

4.3.7. Aktualizacja wykazu „Podatności do natychmiastowego usunięcia".

Wówczas proponowane przez P-PEN podprocesy procesu 4.3.6 metodyki LP-A, zgodnie z numeracją przyjętą dla metodyki LP-A, prezentują się następująco:

- **4.3.6.1 Wstępna analiza**
  - **4.3.6.1.1 Określenie listy spodziewanych ataków**
  - **4.3.6.1.2 Określenie elementarnych ataków**
  - **4.3.6.1.3 Selekcja**
- **4.3.6.2 Badania osiągalności informacji o obiekcie**
- **4.3.6.3 Opracowanie planu testów i przeglądów konfiguracji**
- **4.3.6.4 Akceptacja planu testów i ustalenie zasad szczegółowych i odpowiedzialności**
- **4.3.6.5 Wykonanie badań – testów penetracyjnych**
  - **4.3.6.5.1 Wykonanie właściwych testów penetracyjnych**
- **4.3.6.6 Integracja wyników, opracowanie czarnych scenariuszy i raportu końcowego**

Należy przypomnieć, że poszukiwanie podatności za pomocą narzędzi bezpieczeństwa realizowane jest w odrębnych procesach.

W przypadku, gdy testy penetracyjne realizowane są jako samodzielne przedsięwzięcie, opisane w niniejszym rozdziale procesy należy poprzedzić etapem przygotowawczym, podobnym dla każdego samodzielnego przedsięwzięcia, obejmującym obsługę zapytania ofertowego, umowę, wstępne kontakty formalne ze Zleceniodawcą, rozpoznanie obiektu itd. Podobnie ostatnim etapem (po wymienionych niżej procesach) powinien być końcowy etap rozliczenia pracy – formalne przyjęcie produktu itd. Zobrazowano to na ujętym dla celów ilustracyjnych, nieformalnym diagramie 0 (nieformalny DFD przedsięwzięcia testów penetracyjnych – schemat ogólny).

Tych dodatkowych procesów związanych z organizacją przedsięwzięcia nie opisywano w niniejszym dokumencie, uznając, że wykraczałyby one poza jego zakres tematyczny. Należy jednak zasygnalizować, że procesy organizacyjne przedsięwzięcia są niezwykle ważne ze względów strategicznych, a w przypadku obiektu badań znacznych rozmiarów także bardzo skomplikowane. Np. w dużym projekcie równolegle

do wymienionych niżej procesów powinny być realizowane procesy zarządcze, np. zarządzania, kontroli jakości i bieżącej oceny ryzyka.

Dalej przedstawiono ogólny zapis procesów przedsięwzięcia testów penetracyjnych prowadzonych zgodnie z metodyką P-PEN:

1. Wstępna analiza
   - 1.1. Określenie listy spodziewanych ataków
   - 1.2. Określenie elementarnych ataków
   - 1.3. Selekcja
2. Badania osiągalności informacji o obiekcie
3. Opracowanie planu testów i przeglądów konfiguracji
4. Akceptacja planu testów i ustalenie zasad szczegółowych i odpowiedzialności
5. Wykonanie badań – testów penetracyjnych
   - 5.1. Wykonanie właściwych testów penetracyjnych
   - *5.2. Wykonanie badań automatycznymi narzędziami*
   - *5.3. Wykonanie badań zabezpieczeń technicznych i fizycznych*
6. Integracja wyników, opracowanie czarnych scenariuszy i raportu końcowego

W porównaniu z prezentacją odpowiednich procesów metodyki LP-A można zauważyć, że numery pozbawiono prefiksu „4.3.6." oraz dodano dwa procesy 5.2 i 5.3 (wyróżnione kursywą). Te ostatnie dwa procesy realizowane są w przypadku wykonywania testów penetracyjnych jako samodzielnego przedsięwzięcia (nie w ramach szerszego audytu).

Tab. 1. Zakresy odpowiedzialności i nadzoru nad procesami

Numer procesu	Skrócony opis procesu	Odpowiedzialny	Nadzór
1	Wstępna analiza	AK_1	AK_2
1.1	Określenie listy spodziewanych ataków	AK_1	AK_2
1.2	Określenie elementarnych ataków	SUS-SK	AK_1
1.3	Selekcja	SUS-SK	AK_1
2	Badania osiągalności informacji o obiekcie	AK_1	AK_2
3	Opracowanie planu testów i przeglądów konfiguracji	SUS-SK	AK_1
4	Akceptacja planu testów i ustalenie zasad szczegółowych i odpowiedzialności	AK_1	AK_2
5	Wykonanie badań – testów penetracyjnych	AK_2	AK_1
5.1	Wykonanie właściwych testów penetracyjnych	SUS-SK	AK_1
5.2	*Wykonanie badań automatycznymi narzędziami*	SUS-SK	AK_1
5.3	*Wykonanie badań zabezpieczeń technicznych i fizycznych*	SUS-SK	AK_1
6	Integracja wyników, opracowanie czarnych scenariuszy i raportu końcowego	AK_2	AK_1

Rozdział 4. Specyfikacja dokumentów

W tym rozdziale, metodą IPO (ang. *Input–Process–Output*) są wyspecyfikowane dokumenty związane z prowadzeniem przedsięwzięcia testów penetracyjnych. Na końcu rozdziału, zostały przedstawione dokumenty niezbędne do prowadzenia prac oraz wytwarzane w ich trakcie.

Tabele IPO

Objaśnienia do tabel IPO:

1. Symbol (*) przy numerze procesu oznacza, że proces ten jest dekomponowany na podprocesy.
2. Dokumenty określane w tabelach jako „notatka" dzielą się na dwa rodzaje:
   1) notatki służbowe Zespołu – zapisy autoryzowane, kopie przekazywane Zleceniodawcy
   2) notatki wewnętrzne Zespołu – zapisy nieautoryzowane, bez pozostawiania kopii u Zleceniodawcy.
3. Linią przerywaną zaznaczone są krawędzie tabel zawierających zapisy dotyczące dokumentów lub procesów realizowanych w przypadku prowadzenia testów penetracyjnych jako samodzielnego przedsięwzięcia.

Wejście	• Wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych • Dokumentacja techniczna obiektu • Wewnętrzne regulacje dotyczące porządku prawnego w obiekcie w tym obowiązujące (i praktykowane) procedury • Kategorie ataków
Nr procesu	1*
Proces	Wstępna analiza
Wyjście	• Lista rozważanych ataków kombinowanych • Wykaz elementarnych ataków • Wyselekcjonowana lista ataków do badań ręcznych

Wejście	• Wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych • Dokumentacja techniczna obiektu • Wewnętrzne regulacje dotyczące porządku prawnego w obiekcie w tym obowiązujące (i praktykowane) procedury
Nr procesu	1.1
Proces	Określenie listy spodziewanych ataków
Wyjście	• Lista rozważanych ataków kombinowanych

Wejście	• Lista rozważanych ataków kombinowanych • Dokumentacja techniczna obiektu • Wewnętrzne regulacje dotyczące porządku prawnego w obiekcie

	w tym obowiązujące (i praktykowane) procedury
Nr procesu	1.2
Proces	Określenie elementarnych ataków
Wyjście	• Wykaz elementarnych ataków

Wejście	• Wykaz elementarnych ataków
Nr procesu	1.3
Proces	Selekcja
Wyjście	• Wyselekcjonowana lista ataków do badań ręcznych

Wejście	• Wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych • Dokumentacja techniczna obiektu
Nr procesu	2
Proces	Badania osiągalności informacji o obiekcie
Wyjście	• Notatka służbowa o osiągalności informacji o budowie i właściwościach badanego systemu

Wejście	• Wyselekcjonowana lista ataków do badań ręcznych • Dokumentacja techniczna obiektu
Nr procesu	3
Proces	Opracowanie planu testów i przeglądów konfiguracji
Wyjście	• Plan testów penetracyjnych i przeglądów konfiguracji

Wejście	• Plan testów penetracyjnych i przeglądów konfiguracji
Nr procesu	4
Proces	Akceptacja planu testów i ustalenie zasad szczegółowych i odpowiedzialności
Wyjście	• Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności

Wejście	• Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności • Plan testów penetracyjnych i przeglądów konfiguracji
Nr procesu	5*
Proces	Wykonanie badań – testów penetracyjnych
Wyjście	• Notatki służbowe – sprawozdania z badań i przeglądów konfiguracji • Wstępny wykaz „Podatności do natychmiastowego usunięcia”

	• Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji • Notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż. • Notatka wewnętrzna Zespołu z przeglądu systemu zasilania

Wejście	• Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności • Plan testów penetracyjnych i przeglądów konfiguracji
Nr procesu	5.1
Proces	Wykonanie właściwych testów penetracyjnych
Wyjście	• Notatki służbowe – sprawozdania z badań i przeglądów konfiguracji

Wejście	• Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności • Plan testów penetracyjnych i przeglądów konfiguracji
Nr procesu	5.2
Proces	*Wykonanie badań automatycznymi narzędziami*
Wyjście	• Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji

Wejście	• Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności • Plan testów penetracyjnych i przeglądów konfiguracji
Nr procesu	5.3
Proces	*Wykonanie badań zabezpieczeń technicznych i fizycznych*
Wyjście	• Notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż. • Notatka wewnętrzna Zespołu z przeglądu systemu zasilania

Wejście	• Lista rozważanych ataków kombinowanych • Wyselekcjonowana lista ataków do badań ręcznych • Notatki służbowe – sprawozdania z badań i przeglądów konfiguracji • Wstępny wykaz „Podatności do natychmiastowego usunięcia” • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji • Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji • Notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż. • Notatka wewnętrzna Zespołu z przeglądu systemu zasilania • Notatka służbowa o osiągalności informacji o budowie i właściwościach badanego systemu
Nr procesu	6
Proces	Integracja wyników
Wyjście	• Wykaz „Podatności do natychmiastowego usunięcia” • Raport z testów penetracyjnych (wyniki ręcznych testów penetracyjnych)

Specyfikacja zbiorcza dokumentów

Podobnie jak w przypadku tabel IPO, dalej wymieniono tylko dokumenty podstawowe dotyczące testów penetracyjnych, pomijając dokumenty związane z organizacją przedsięwzięcia. Z dokumentów niezbędnych do przeprowadzenia prac dotyczących obiektu (badanego systemu Zleceniodawcy) wymieniono dwa:

1. Dokumentacja techniczna obiektu;
2. Wewnętrzne regulacje dotyczące porządku prawnego w obiekcie w tym obowiązujące (i praktykowane) procedury;

istotnym narzędziem zespołu jest wykaz rodzajów ataków, aktualny na dzień rozpoczęcia testów:

3. Kategorie ataków.

Tab. 1. Wykaz wytwarzanych dokumentów

Lp.	Nazwa dokumentu	Status dokumentu	Wytwórca
1. (15)	Notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż.	Wewnętrzny	Eksperci
2. (16)	Notatka wewnętrzna Zespołu z przeglądu systemu zasilania	Wewnętrzny	Eksperci
3. (22)	Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności	Wewnętrzny	Eksperci

4. (23)	Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji	Wewnętrzny	Eksperci
5. (27)	Raport z badań technicznych systemów i sieci teleinformatycznych Zleceniodawcy	Wewnętrzny	Eksperci
6. (24)	Notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji	Wewnętrzny	Eksperci
7. (25)	Wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych	Wewnętrzny	Wykonawcy
8. ---	Lista rozważanych ataków kombinowanych	Wewnętrzny	Wykonawcy
9. ---	Wykaz elementarnych ataków	Wewnętrzny	Wykonawcy
10. ---	Wyselekcjonowana lista ataków do badań ręcznych	Wewnętrzny	Eksperci
11. ---	Notatka służbowa o osiągalności informacji o budowie i właściwościach badanego systemu	Wewnętrzny	Wykonawcy
12. ---	Plan testów penetracyjnych i przeglądów konfiguracji	Oficjalny/przek.	Wykonawcy
13. ---	Oświadczenie zleceniodawcy o akceptacji planu testów i zasadach odpowiedzialności	Oficjalny	Zleceniodawca
14. ---	Notatki służbowe – sprawozdania z badań i przeglądów konfiguracji	Oficjalny	Eksp./Zlec.
15. (26)	Wstępny wykaz „Podatności do natychmiastowego usunięcia”	Wewnętrzny	Wykonawcy
16. (28)	Raport z testów penetracyjnych (wyniki ręcznych testów penetracyjnych)	Oficjalny/przek.	Wykonawcy
17. (29)	Wykaz „Podatności do natychmiastowego usunięcia”	Oficjalny/przek.	Wykonawcy
18. (30)	Potwierdzenie przez Zleceniodawcę przyjęcia wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia”	Oficjalny	Wyk./Zlec.
19. (32)	Wybrane raporty generowane przez narzędzia	Oficjalny	Wykonawcy

UWAGI

1. Numery w nawiasach okrągłych w kolumnie „Lp.” oznaczają numery odpowiednich dokumentów według wykazu metodyki LP-A.
2. Nazewnictwo dokumentów odpowiada użytemu w LP-A z wyjątkiem wiersza 16, gdzie nazwę odpowiednika dokumentu wg LP-A ujęto w nawiasie.
3. Opis Wyk./Zlec. lub Eksp./Zlec. w kolumnie „Wytwórca” oznacza, że jest to dokument wytwarzany w wyniku wzajemnych uzgodnień pomiędzy wykonawcami i upoważnionymi przedstawicielami Zleceniodawcy, autoryzowany przez obie strony.
4. Status „oficjalny/przek.” oznacza, że dokument ten zostaje przekazany zleceniodawcy w trakcie prac.
5. Status „oficjalny” oznacza, ze dokument ten stanowi bezpośrednią podstawę do opracowania dokumentów końcowych lub zostaje do tych dokumentów włączony w całości.
6. W kolumnie „Wytwórca” zamiast „wykonawcy” używano określenia „eksperci”.

Rozdział 5. Diagramy przepływu danych

Na podstawie zamieszczonych w dalszej części diagramów można:
1) ocenić złożoność procesów;
2) rozpoznać zależności pomiędzy dokumentami;
3) ocenić na podstawie zależności pomiędzy procesami oraz składu osobowego Zespołu, możliwości równoległego prowadzenia zadań.

Dla Zleceniobiorcy, diagramy (i metodyka jako całość) znacznie wspomaga wycenę prac. Należy przy tym zaznaczyć, że w przypadku przedsięwzięcia w Instytucji posiadającej rozłożone terytorialnie Oddziały i Filie (lub podobne jednostki organizacyjne), przedstawione procesy etapu wykonawczego będą powielane. W przypadku posiadania przez Zespół wystarczających zasobów ludzkich i odpowiednich narzędzi, jeżeli tego wymaga konkretny kontrakt, istnieje możliwość zrównoleglenia znacznej części prac.

Rozdział 6. Rzetelne praktyki

Niniejszy rozdział zawiera zapis tzw. „rzetelnych praktyk" (nazywanych też „najlepszymi praktykami" – z ang. *best practices*), tj. należących do kategorii know-how, heurystycznych metod postępowania, wypracowanych i sprawdzonych podczas dotychczasowej praktyki.

1. Każde badanie, rozmowa, wizja lokalna etc. jest zawsze przeprowadzana przez dwóch członków Zespołu.
2. Z każdego działania – badania, rozmowy, wizji lokalnej etc. jest sporządzana notatka wewnętrzna, która może być autoryzowana, w razie potrzeby, przez drugą stronę (w dokumentach Zespołu, podlegające autoryzacji notatki wewnętrzne są nazywane notatkami służbowymi).
3. Szkolenie wewnętrzne Zespołu – specjalista od sieci i urządzeń sieciowych (członek zespołu) prezentuje zespołowi ogólny model przepływu informacji w sieci lub sieciach, w tym rozdział stref dystrybucji pakietów i zainstalowane mechanizmy separujące.
4. Wszelkie działania inwazyjne w systemach Zleceniodawcy realizowane są przez uprawnionych pracowników Zleceniodawcy pod kierunkiem członków zespołu. Członkowie zespołu wykonawcy nie przejmują odpowiedzialności kompetentnych pracowników Zleceniodawcy w żadnym zakresie, nawet jeśli dla przyspieszenia prac zostaną dopuszczeni do występowania w roli operatora. Przy ortodoksyjnym traktowaniu tej zasady, podczas badań członkowie zespołu fizycznie nie będą w ogóle dotykać żadnych urządzeń.
5. Wszelkie przeglądy (np. konfiguracji stacji roboczych) są wykonywane przez członków zespołu zawsze w asyście przedstawiciela Zleceniodawcy (np. administratora stacji roboczych) i za jego zgodą.
6. W przypadku wykrycia szczególnie groźnych podatności podczas badań technicznych, Zleceniodawca jest informowany o nich **natychmiast** po ich wykryciu, bez oczekiwania na zakończenie całości prac. Postępowanie takie pozwala Zleceniodawcy na podjęcie bezzwłocznych działań mających na celu ochronę (przed wykorzystaniem przez zagrożenia istniejących i wykrytych podatności) informacji przetwarzanej, przechowywanej i przesyłanej w jego systemach i sieciach teleinformatycznych.

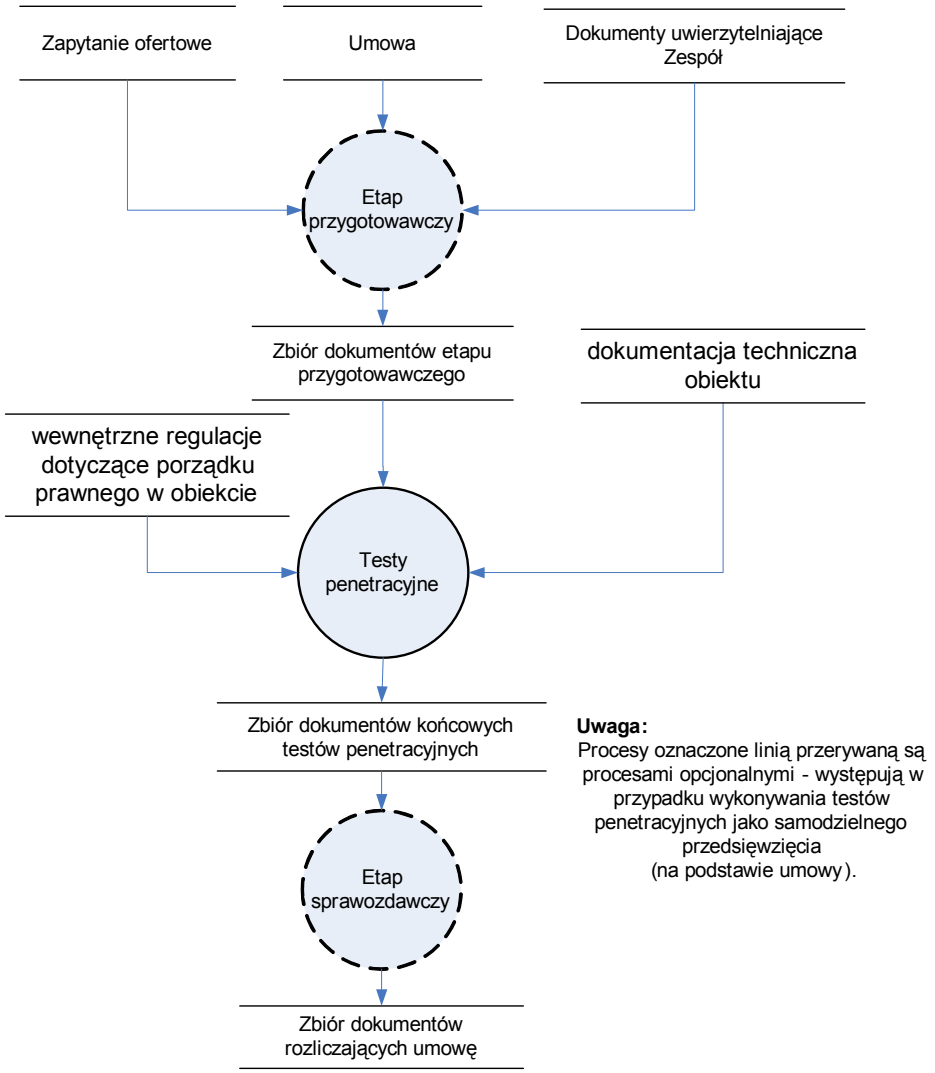


Diagram 5.1. Nieformalny DFD samodzielnego przedsięwzięcia testów penetracyjnych

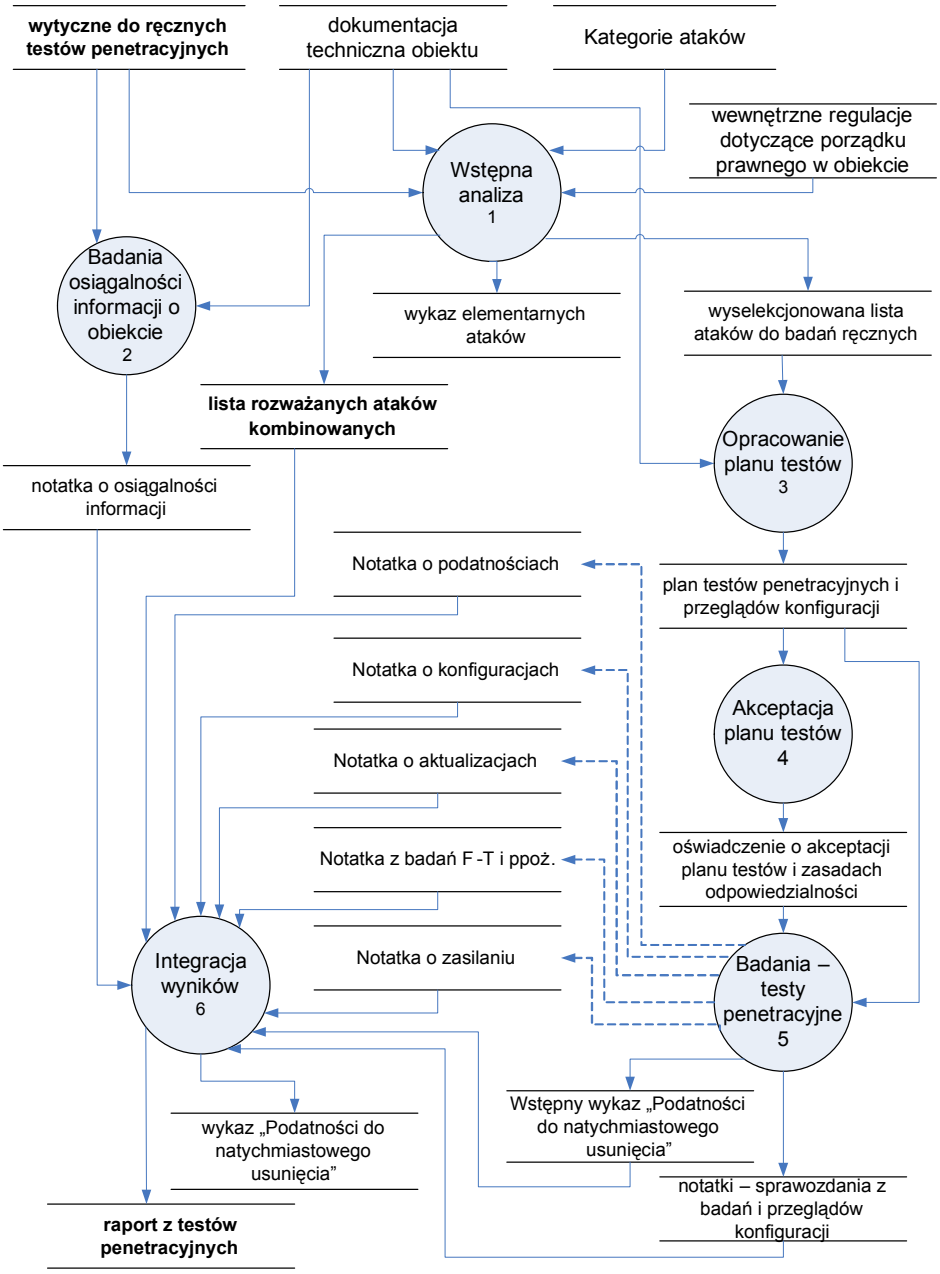


Diagram 5.2. DFD_1 testów penetracyjnych – schemat ogólny.

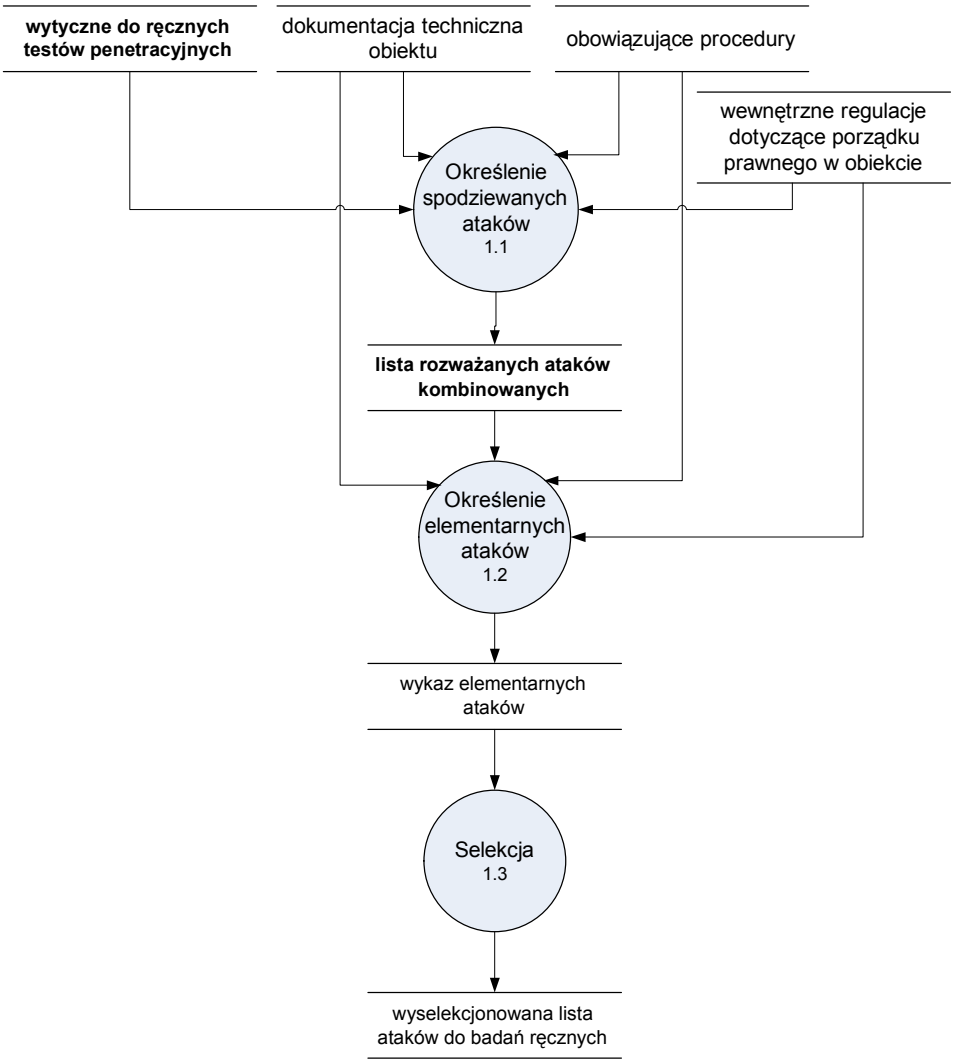


Diagram 5.3. DFD_2 fazy analizy – proces nr 1

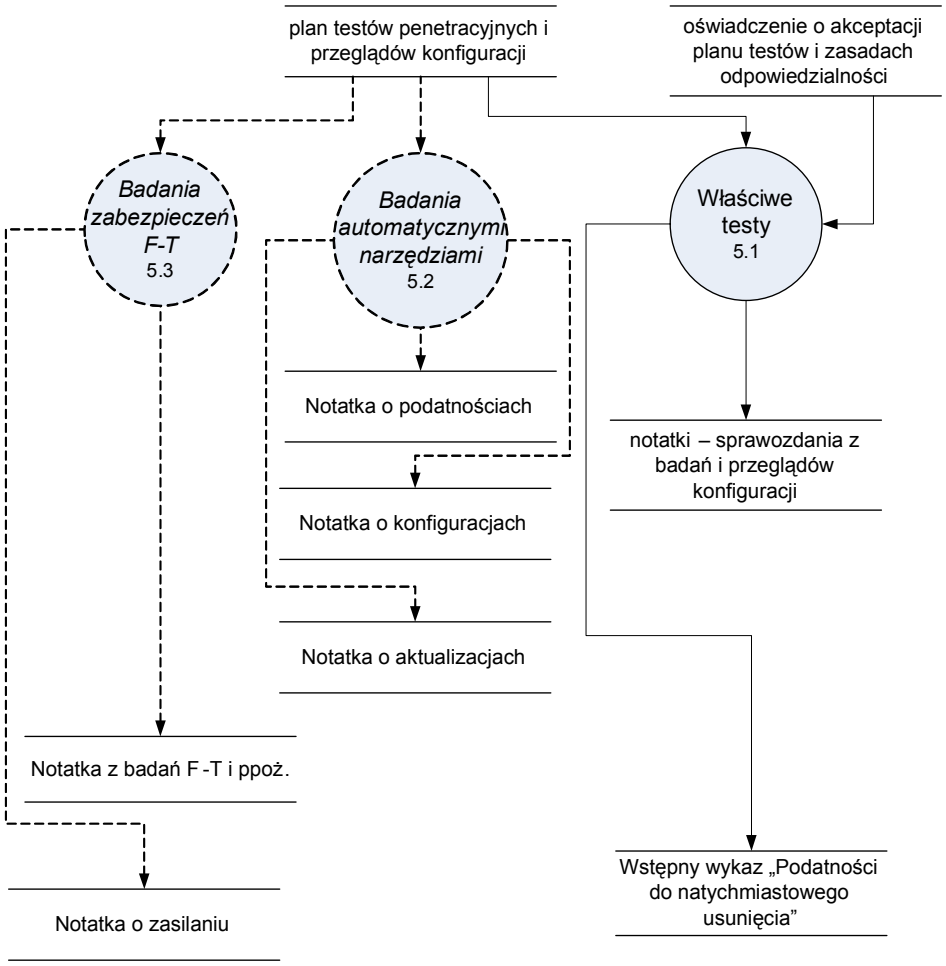


Diagram 5.4. DFD_2 proces nr 5

Rozdział 7. Kategorie ataków

Zbiór kategorii ataków, to lista możliwych rodzajów ataków, wyczerpująca repertuar znanych i stosowalnych ataków, formułowana według stanu wiedzy aktualnego na pewien dzień (najlepiej na dzień rozpoczęcia audytu lub testów penetracyjnych). Celem wykorzystywania tej listy jest wymuszenie pewnej dyscypliny na pracownikach formułujących spis możliwych ataków. Chodzi o zapewnienie, że poświęcą oni każdej z kategorii uwagę, chociażby po to, aby odpowiedzialnie stwierdzić, że w badanym

obiekcie ataki pewnej kategorii nie są możliwe. Rozsądne jest przeprowadzenie sesji przeglądu kategorii ataków w formie moderowanej sesji, w której rola moderatora sprowadza się do wymuszania kolejnych kroków według listy kategorii ataków i zadawania pytań obowiązkowych. Poza tym każda kategoria omawiana jest zgodnie z regułami burzy mózgów.

Rozsądne jest rozpatrywanie zespół ekspertów takich kategorii określając przy rozpatrywaniu każdej odpowiedzi na pytania:

- Czy w systemie znajdują się fragmenty, dla których rozważana kategoria znajduje zastosowanie?
- Czy można wskazać scenariusz (także „czarny scenariusz") ataku kombinowanego, przynoszącego szkodę Zleceniodawcy, a zawierający ataki rozważanej kategorii?
- Jakie mogą być miejsca, z których ataki rozpatrywanej kategorii można przeprowadzić (wewnętrzne, zewnętrzne)?

Poniżej zaprezentowano przykład wykazu kategorii ataków:

1. Ataki prowadzące do odmowy usług DoS (Denial-of-Service).
   - 1.1. Nadużycia własności usługi lub protokołu.
     - 1.1.1. Zasypywanie kont pocztowych (e-mail) przesyłkami – mailbombing.
     - 1.1.2. Zalewanie pakietami – flooding.
     - 1.1.3. Przepełnianie tablicy półotwartych połączeń serwera TCP (SYN-flooding).
     - 1.1.4. Zajęcie całej puli DHCP.
     - 1.1.5. Przekroczenia wartości granicznych różnych parametrów technicznych protokołów.
     - 1.1.6. Atak na routing (wstrzeliwanie fałszywych pakietów protokołu routingu)
     - 1.1.7. …
   - 1.2. Wykorzystania znanych wad produkcyjnych (bugs) oprogramowania badanego systemu.
   - 1.3. Przeciążanie systemów analizy treści przez zmuszanie ich do buforowania wielkich jednostek informacji (np. kolejne wielkie przesyłki zawierające archiwa zip, nadsyłane bez ostatniego pakietu, blokujące systemy antywirusowe, zwykle poczty, na wejściu sieci firmowej).
   - 1.4. …
2. Przenikanie filtrów sieciowych.
   - 2.1. Wykorzystanie nienadzorowanego ruchu.
   - 2.2. Tunelowanie kryptograficzne.
   - 2.3. Ustanowienie ukrytych kanałów.
   - 2.4. Ustanowienie kanałów zwrotnych (zza NAT – Network Address Translation).
   - 2.5. …
3. Podsłuch ruchu sieciowego.
   - 3.1. Podsłuchiwanie – sniffing.
   - 3.2. Przekierowanie ruchu – ARP-spoofing dla podsłuchu w sieciach ze switchami.
   - 3.3. Atak Man-In-The-Middle (MITM) na protokoły połączeniowe, ustanowienie proxy lub innego mechanizmu przekazywania ruchu sieciowego.
   - 3.4. MITM dzięki fałszywemu serwerowi DHCP – wskazanie fałszywej bramki domyślnej
   - 3.5. VLAN hopping.
   - 3.6. Podsłuch łączy.
   - 3.7. Podsłuch sieci bezprzewodowej.

3.8. Podsłuch urządzeń bezprzewodowych.
3.9. Wykorzystanie keyloggerów.
3.10. …

4. Przejęcia sesji.
   4.1. W sieci wewnętrznej – specyficznych aplikacji.
   4.2. Webowych przez podszywanie się (m.in. manipulacja cookies).
   4.3. …
5. Kryptoanaliza
   5.1. Zdobywanie materiału do kryptoanalizy i kryptoanaliza off-line
   5.2. Ataki kryptoanalityczne on-line
   5.3. Zdobycie kluczy VPN
   5.4. Zdobycie uprawnień generalnych w sieciach MS Windows
   5.5. Wykorzystanie haseł domyślnych – ustawianych fabrycznie
   5.6. …
6. Ataki lokalne na stacje robocze.
   6.1. Eskalacja uprawnień użytkownika (techniki specyficzne dla systemu operacyjnego: błędy konfiguracji, przepełnienia bufora, rootkits itd.).
   6.2. Osadzenie automatycznych narzędzi szpiegujących.
      6.2.1. Skryta, ręczna modyfikacja oprogramowania stacji.
      6.2.2. Nakłonienie operatora do instalacji.
      6.2.3. Nakłonienie personelu technicznego do instalacji (np. jako poprawki).
   6.3. Nieuprawniony dostęp do zasobów stacji przez operatora.
   6.4. …
7. Ataki wewnętrzne na zasoby sieci lokalnej.
   7.1. Z przejętego poza siecią komputera przenośnego.
   7.2. Włączenie przez intruza obcego komputera w sieci wewnętrznej (niedostateczny nadzór nad gniazdkami sieciowymi).
   7.3. Przez przyłączenie spreparowanego nośnika (np. CD, pamięci flash).
   7.4. Atak legalnego operatora, przekroczenie uprawnień z sąsiedniej stacji roboczej.
      7.4.1. Wykorzystanie kont wspólnych (np. lokalnego operatora w sieciach Windows).
      7.4.2. Wykorzystanie błędów konfiguracji.
      7.4.3. Wykorzystanie specyficznych klientów aplikacji.
   7.5. Wykorzystanie znanych wad produkcyjnych oprogramowania (bugs).
   7.6. …
8. Ataki na aplikacje
   8.1. Atak na bazę danych za pośrednictwem interfejsu WWW.
      8.1.1. SQL injection.
      8.1.2. …
   8.2. Wykorzystanie łańcuchów formatujących (format strings).
   8.3. Przepełnienia bufora.
   8.4. Wykorzystanie znanych wad produkcyjnych oprogramowania (bugs).
   8.5. …
9. Ataki na aplikacje specyficzne dla badanego systemu.
   9.1. Lokalne ataki na klienta aplikacji.
   9.2. Zdalne ataki na serwer aplikacji.
   9.3. Wykorzystanie typowych błędów programistów.
   9.4. …
10. Skierowanie mechanizmów ochronnych przeciw elementom systemu („atak HIV").

10.1. Blokada kont usługi po wielokrotnych próbach logowania z błędnym hasłem.
10.2. Przekroczenie dopuszczalnych rozmiarów logów (także zapełnienie dysku logami).
10.3. Spowodowanie wygenerowania dynamicznych reguł filtrów sieciowych (np. firewalli) przez generowanie ruchu sieciowego zawierającego rozpoznawane sygnatury ataków i fałszywe identyfikatory źródeł ruchu.
10.4. Przeciążanie systemu wewnętrznym ruchem generowanym przez rozproszony system wykrywania włamań (IDS).
10.5. …

11. Znane exploity zidentyfikowanych elementów programowych obiektu (jeśli nie są sprawdzane w ramach badań automatycznych). Należy rozpatrzyć exploity ostatnio opublikowane w powszechnie uznanej witrynie, o krótkim czasie aktualizacji, np.:
11.1. http://www.securiteam.com/exploits/archive.html
11.2. http://packetstormsecurity.nl/
11.3. …
12. Manipulowanie ludźmi (social engineering)
12.1. Typowe techniki werbowania (w tym „pod fałszywą flagą").
12.2. Podrzucenie nośników.
12.3. Wyłudzanie danych autentykacyjnych.
12.4. Nakłanianie do „niewielkich grzeczności".
12.5. Wykorzystanie przeciw pracownikom kompromitujących informacji wydobytych z ich stacji roboczych.
12.6. …