

Podstawowe zasady realizacji testów penetracyjnych systemu informatycznego

Opracował: Mariusz Stawowski

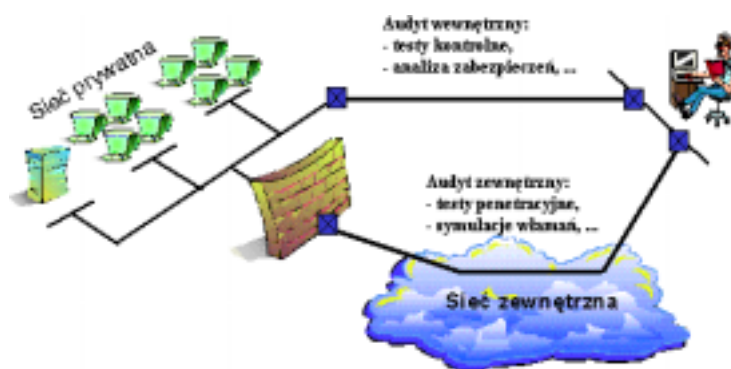
Utrzymywanie wysokiego poziomu bezpieczeństwa systemu informatycznego wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów tego systemu. Nawet najbardziej zaawansowany system ochrony, który w trakcie eksploatacji nie jest poddawany odpowiedniej weryfikacji szybko traci swoje właściwości i sam może stać się źródłem zagrożenia. Użytkownicy przeświadczeni o istnieniu zabezpieczeń nie odczuwają niebezpieczeństw i mogą narazić swoją organizację na poważne straty (np. utratę poufności tajnych informacji firmy przesyłanych za pośrednictwem szyfrowanych łączy komunikacyjnych, które w wyniku awarii nie zabezpieczają transmisji danych). Nieprawidłowe funkcjonowanie systemu ochrony jest z reguły trudne do wykrycia, ponieważ większość zabezpieczeń jest przezroczysta dla użytkowników systemu. W związku z tym wymagane jest wyposażenie systemu informatycznego w środki szybkiego identyfikowania i sygnalizowania nieprawidłowego działania zabezpieczeń oraz wykonywanie okresowych audytów bezpieczeństwa.

Występują trzy podstawowe metody oceny stanu technicznego zabezpieczenia zasobów systemu informatycznego: testy penetracyjne (identyfikacja słabych punktów systemu zabezpieczeń, symulacja włamań), testy kontrolne (sprawdzanie poprawności instalacji i konfiguracji systemu) oraz analiza systemowa zabezpieczeń (teoretyczna ocena bezpieczeństwa systemu informatycznego).

Testy penetracyjne są podstawowym sposobem analizy bezpieczeństwa systemu informatycznego. Celem ich realizacji jest dokonanie praktycznej oceny poziomu bezpieczeństwa zasobów informatycznych systemu w zdefiniowanej przez Zleceniodawcę części pod kątem szczelności i odporności na nieupoważnione ingerencje w działanie systemu z obszaru sieci wewnętrznej i Internetu.

Zakres realizowanych kompleksowo testów obejmuje następujące etapy prac:

- I. testy penetracyjne zewnętrzne,
- II. testy penetracyjne wewnętrzne.



Podczas wykonywania testów penetracyjnych należy liczyć się z możliwością zakłócenia poprawnej pracy systemu informatycznego, a nawet zniszczenia jego danych. Z tych powodów system powinien zostać wcześniej odpowiednio zabezpieczony (np. poprzez wykonanie pełnych kopii Backup). Zagrożenie uszkodzenia systemu nie powinno być jednak czynnikiem wymuszającym zbyt „ostrożne” i tym samym mało wiarygodne testy.

Zewnętrzne testy penetracyjne

Zewnętrzne testy penetracyjne są wykonywane w pierwszej kolejności z wykorzystaniem popularnych technik i narzędzi hackerskich. Zalecane jest, aby uzyskane wyniki testów zostały dodatkowo zweryfikowane za pomocą komercyjnych skanerów zabezpieczeń (np. ISS Internet Scanner, WebTrends Security Analyzer). Hakerzy z Internetu łamiąc kody licencji są w posiadaniu takich skanerów (patrz <http://www.thecrack.net>).

Zewnętrzne testy penetracyjne obejmują następujące prace:

1. **Identyfikacja systemu za pomocą dostępnych serwisów sieciowych (np. WWW, SMTP, FTP, Telnet).**
2. **Rozpoznanie dostępnych z obszaru Internetu komputerów i urządzeń sieciowych, rodzaju i wersji systemów operacyjnych oraz oprogramowania użytkowego pod kątem wykrywania znanych luk bezpieczeństwa.**
3. **Wstępna penetracja systemu za pomocą skanerów portów TCP i UDP oraz skanerów zabezpieczeń powszechnie stosowanych przez hakerów, dostępnych w zasobach sieci Internet.**
4. **(opcjonalnie) Testy zabezpieczeń systemu za pomocą profesjonalnych skanerów zabezpieczeń ISS Internet Scanner lub WebTrends Security Analyzer.**
5. **Analiza topologii sieci komputerowej widzianej z Internetu.**
6. **Analiza otrzymanych wyników pod kątem przygotowania symulacji włamań.**
7. **Symulacja włamań.**
8. **Ocena odporności zabezpieczeń systemu na ataki destrukcyjne za pomocą narzędzi dostępnych w zasobach sieci Internet.**
9. **Ocena poprawności reakcji systemu zabezpieczeń na wykonywane ataki.**
10. **Analiza bezpieczeństwa systemu zaporowego Firewall.**
11. **Analiza wyników testu penetracyjnego pod kątem oceny zagrożenia integralności systemu oraz możliwości dostępu do danych przez osoby nieupoważnione.**
12. **Analiza dokumentacji systemu pod kątem bezpieczeństwa (struktura sieci, konfiguracja, zastosowane urządzenia i oprogramowanie).**

Analiza bezpieczeństwa wykonywana jest w ścisłej współpracy z administratorami testowanych systemów. Jest to szczególnie istotne w trakcie wykonywania badań odporności systemu na ataki destrukcyjne oraz symulację włamań, a także poprawności reakcji zabezpieczeń na wykonywane ataki. Kadra informatyczna zaangażowana w realizację przedsięwzięć bezpieczeństwa powinna zostać odpowiednio do tego celu przeszkolona.

Wynikiem testów penetracyjnych jest raport opisujący rzeczywisty stan zabezpieczenia zasobów systemu informatycznego. Dla wszystkich wyznaczonych „słabych punktów” zabezpieczeń systemu przedstawione zostają dokładne procedury ich eliminacji, bądź redukcji. Dokumentacja z realizacji audytu zawiera szczegółowy opis wszystkich wykonanych testów (m.in. zastosowane narzędzia, sposób uruchamiania testów).

Test penetracyjny rozpoczyna się najczęściej od zebrania informacji na temat obiektu badań bez nawiązywania bezpośredniego kontaktu z tym obiektem. Można tego dokonać np. poprzez analizowanie systemu nazw domenowych DNS, uzyskanie danych zarejestrowanych u dostawcy usług internetowych oraz przeszukiwanie innych publicznych zbiorów informacji (np. rejestr RIPE, serwis WWW, katalogi LDAP). Następnie wykonywane są próby uzyskania dostępu do zasobów badanego systemu z wykorzystaniem zdobytych wcześniej informacji. Ma to na celu sprawdzenie odporności systemu na atak, który nie został poprzedzony starannym okresem przygotowawczym. Z takimi atakami mamy do czynienia na co dzień, kiedy to hakerzy penetrując zasoby Internetu natrafiają na nowy system i od razu przystępują do jego zagarnięcia.

Zewnętrzne testy penetracyjne ukierunkowane są na typowe zagrożenia dla systemu informatycznego wynikające z podłączenia do Internetu:

- **Exploits** – uzyskanie nieupoważnionego dostępu do systemu poprzez wykorzystanie podatności systemu (np. błędów oprogramowania, konfiguracji), m.in.:
 - Niewłaściwe prawa dostępu – wykorzystanie niewłaściwych ustawień praw dostępu do usług i informacji,
 - Atak na hasła (np. RAS, VPN) – próba uzyskania dostępu do systemu poprzez podawanie haseł w formie kolejnych kombinacji znaków, wykorzystanie słownika haseł, bądź tzw. słabych haseł (specyficznych dla określonych systemów),
 - Przepełnienie bufora – doprowadzenie do przepełnienia bufora aplikacji połączone z wprowadzeniem do bufora odpowiedniego kodu (np. poleceń systemowych) i uruchomienie tego kodu,
 - Specyficzne Exploits – uzyskanie nieupoważnionego dostępu do usług i informacji serwera sieciowego poprzez wykorzystanie specyficznych błędów tego serwera,
 - Niestabilność systemu (ang. race condition) – próba uzyskania dostępu do systemu poprzez wykorzystanie tymczasowej niestabilności systemu spowodowanej np. uruchomieniem określonej aplikacji.
- **D/DoS** – zakłócenie, bądź zablokowanie usług systemu informatycznego, m.in.:
 - Flooding – wysyłanie dużej liczby pakietów (zapytań, danych),
 - Smurfing – zwielokrotnienie ataku Flooding poprzez użycie IP Broadcasts i IP Spoofing,
 - IP Fragmentation Attacks – wykorzystanie błędów implementacji stosu TCP/IP,
 - SYN Flooding – wysyłanie dużej liczby zapytań SYN w imieniu nie istniejącego klienta TCP (IP Spoofing),
 - Nuking – wysyłanie specjalnie spreparowanych pakietów ICMP i TCP w celu zamknięcia aktywnego połączenia sieciowego,
 - Specyficzne DoS – wysyłanie zapytań blokujących usługi serwera sieciowego poprzez wykorzystanie specyficznych błędów tego serwera.

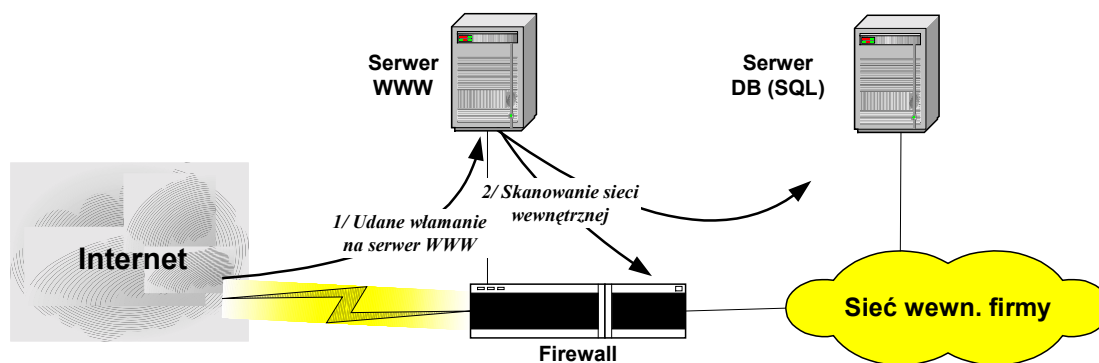
Inną kategorię istotnych zagrożeń dla systemu informatycznego stanowią wirusy, robaki, konie trojańskie i inne groźne aplikacje. Zagadnienia te są zwykle analizowane w trakcie wewnętrznej analizy bezpieczeństwa, ponieważ z zewnątrz trudno jest dokonać oceny rzeczywistych skutków tego zagrożenia.

Scenariusz symulacji włamań

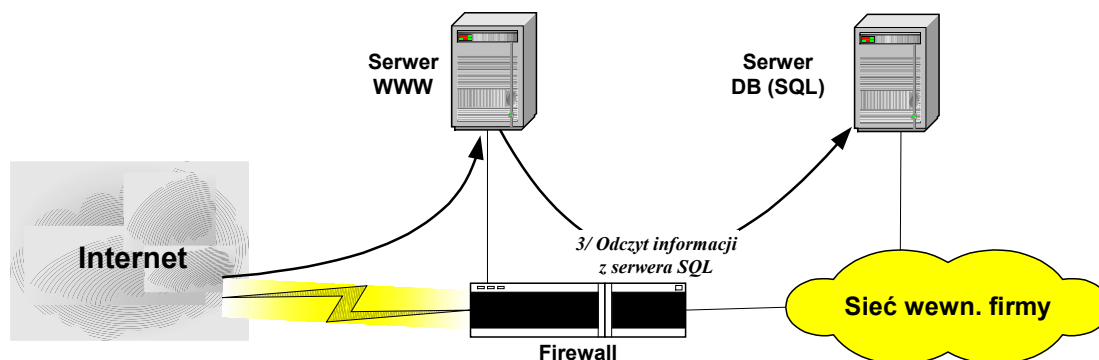
Symulacja włamań odbywa się na analogicznych zasadach jak robią to hakerzy. Obserwowane w Internecie ataki hakerów zwykle rozpoczynają się od penetracji i przejęcia kontroli nad serwerem publicznym firmy (np. Web, SMTP, DNS). Serwery takie w większości firm znajdują się w wydzielonym segmencie sieci tzw. DMZ. Wykonanie włamań na serwer jest możliwe, gdy oprogramowanie tego serwera posiada błąd umożliwiający uruchamianie poleceń systemowych. Można w ten sposób skopiować na serwer aplikację typu Trojan (np. NetCat, NetBus, BO, SubSeven) i uruchomić ją w celu uzyskania zdalnego dostępu do systemu. Błąd oprogramowania serwera implementowany jest zwykle w specjalnej aplikacji, popularnie nazywanej Exploit. Po przejęciu kontroli nad serwerem haker może wykonywać na nim różnego rodzaju działania (np. Web graffiti) lub kontynuować atak na inne strefy bezpieczeństwa (np. sieć wewnętrzną). Taktyka przejmowania kontroli nad kolejnymi strefami bezpieczeństwa w sieci nosi nazwę *Island Hopping Attack*.

Scenariusz typowego włamań do sieci wewnętrznej firmy poprzez Exploit przebiega w następujący sposób:

1. Penetracja i przejęcie kontroli nad serwerem w strefie DMZ.
2. Skanowanie sieci wewnętrznej.



3. Odczyt i modyfikacje informacji z serwera w sieci wewnętrznej oraz inne próby penetracji.



Zasady kontrolowanego badania szczelności i efektywności zabezpieczeń systemu informatycznego

Proces przygotowania do realizacji testów penetracyjnych i symulacji włamań przebiega w następujący sposób:

1. Ustalenie celu analizy i uzyskanie jego akceptacji przez Zleceniodawcę.
2. Ustalenie zakresu analizy i uzyskanie jego akceptacji przez Zleceniodawcę:
 - a. komputery i urządzenia sieciowe

Należy dokładnie sprecyzować adresy (IP, nr telefonów), które będą poddawane badaniom oraz upewnić się, że są one własnością Zleceniodawcy.

- b. usługi i protokoły sieciowe wyłączone z badań

W razie potrzeby należy ustalić ze Zleceniodawcą usługi i protokoły sieciowe, które nie powinny być poddawane testom. Zalecane jest, aby testy dla których istnieje zagrożenie zakłócenia pracy systemu (np. elementy symulacji włamań, badanie odporności na DoS) były wykonywane we współpracy z administratorami systemów.

3. Ustalenie harmonogramu realizacji prac i uzyskanie jego akceptacji przez Zleceniodawcę.

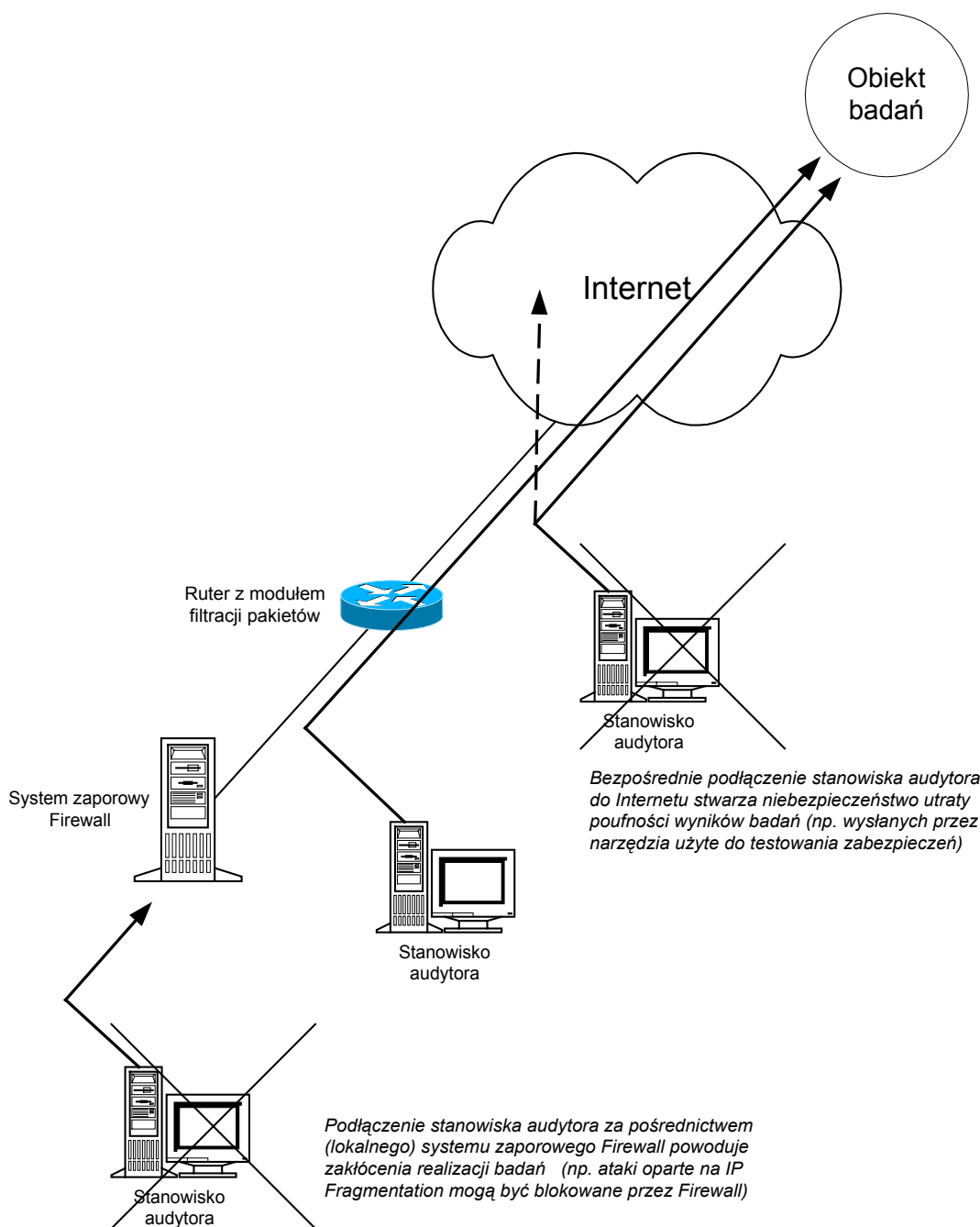
Harmonogram prac powinien uwzględniać czas przeznaczony na przygotowanie dokładnego planu badań (m.in. symulacji włamań), przygotowanie stanowisk do testowania, skompletowanie i zweryfikowanie narzędzi, szkolenie administratorów (w razie potrzeby), wykonanie badań, analizę wyników oraz sporządzenie raportu końcowego i dokumentacji.

4. Ustalenie zasad współpracy z administratorami badanych systemów.

Współpraca zespołu audytorów z administratorami systemów jest bardzo istotna, szczególnie w czasie wykonywania testów inwazyjnych oraz w trakcie badania poprawności reakcji zabezpieczeń systemów na ataki.

5. Przygotowanie stanowisk do testowania.

Stanowiska do testowania powinny być zlokalizowane w miejscach umożliwiających wiarygodne i bezpieczne wykonywanie badań (patrz rysunek).



6. Skompletowanie i przetestowanie narzędzi do testowania.

W pierwszym etapie audytu wykorzystywane są narzędzia ogólnie dostępne w Internecie (tzw. programy hakerskie). Zalecane jest, aby sprowadzić aktualne wersje tego typu programów, wyszukane pod kątem systemów przewidzianych do badania (np. skanery dla NT, Linux). Wyniki uzyskane za pomocą niekomercyjnych skanerów (np. Nessus, Saint) powinny zostać zweryfikowane za pomocą profesjonalnego oprogramowania (np. ISS Internet Scanner, WebTrends Security Analyzer). Do wykorzystania komercyjnych skanerów zabezpieczeń wymagane jest wcześniejsze uzyskanie licencji (na określone adresy IP).

Wewnętrzne testy penetracyjne

Wewnętrzne testy penetracyjne odbywają się z sieci na podobnych zasadach jak testy zewnętrzne. Podstawowe badania wykonywane zabezpieczeń odbywają się także bezpośrednio na testowanych urządzeniach. Testy wewnętrzne wykonuje się za pomocą komercyjnych skanerów zabezpieczeń (np. ISS Internet Scanner, WebTrends Security Analyzer) oraz innych dostępnych narzędzi administracyjnych i diagnostycznych.

Wewnętrzne testy penetracyjne ukierunkowane są na następujące aspekty bezpieczeństwa:

1. Analiza bezpieczeństwa sieci (m.in. sprawdzenie jak prezentuje się sieć organizacji od wewnątrz, jakie rodzaje systemów operacyjnych są stosowane, jakie usługi udostępniają, jakie urządzenia sieciowe znajdują się wewnątrz organizacji, jakie zastosowano systemy zabezpieczeń).
2. Weryfikacja poprawności konfiguracji elementów sieciowych systemu informatycznego.
3. Próby przechwytywania przesyłanych wewnątrz sieci niewrażliwych informacji (konta, hasła, dane itp.).
4. Sprawdzenie możliwości nieupoważnionego dostępu do danych.
5. Analiza topologii i struktury sieci w kategoriach wydajnościowych i niezawodnościowych.
6. Przeanalizowanie poziomu bezpieczeństwa istniejących serwerów usług:
 - próba nieupoważnionego uzyskania wyższych uprawnień w systemie informatycznym,
 - analiza możliwości destabilizacji pracy sieci wewnętrznej.
7. Atak za pomocą programu typu "Koń trojański":
 - analiza i praktyczna weryfikacja możliwości ataku przez pocztę elektroniczną, FTP i HTTP (transfer pliku, ActiveX),
 - analiza i praktyczna weryfikacja możliwości przejęcia kontroli nad stacją roboczą w sieci wewnętrznej oraz penetracji sieci wewnętrznej.

Wyniki analizy bezpieczeństwa

Zasadniczym rezultatem analizy bezpieczeństwa jest raport opisujący rzeczywisty stan zabezpieczenia zasobów systemu informatycznego.

Oprócz tego audyt dostarcza wielu innych korzyści, m.in.:

- kadra informatyczna zaangażowana w realizację przedsięwzięć bezpieczeństwa zostaje odpowiednio do tego celu przeszkolona i zdobywa duże doświadczenie,
- dla wszystkich wyznaczonych „słabych punktów” zabezpieczeń systemu informatycznego przedstawione zostają procedury ich eliminacji, bądź redukcji,
- dokumentacja z realizacji audytu bezpieczeństwa zawiera szczegółowy opis wszystkich wykonanych testów (m.in. zastosowane narzędzia, sposób uruchamiania testów) i dzięki temu w przyszłości może posłużyć do powtórzenia lub zweryfikowania badań.

Wyniki analizy bezpieczeństwa stanowią podstawę do opracowania projektu rozwoju, bądź poprawy zabezpieczeń systemu informatycznego.