Testy Penetracyjne

Raportowanie

Arkadiusz Chrobot

Katedra Systemów Informatycznych

29 maja 2024

Plan

Wstęp

Głównym powodem, dla którego firmy, instytucje i organizacje zlecają wykonanie testów penetracyjnych jest potrzeba oceny stanu zabezpieczeń ich systemów informatycznych, a w szczególności poznania istniejących w nich słabych punktów. Przyczyn powstania takiej potrzeby jest zwykle kilka, ale aby została ona spełniona musi sprawnie funkcjonować komunikacja między stroną zamawiającą testy, a ich wykonawcą. Nie może się ona ograniczać jedynie do przekazania sprawozdania z zakończonych prac. Informacja musi być przekazywana między obiema stronami także w trakcie ich trwania, a nawet po ich zakończeniu, w ramach działań uzupełniających.

Komunikacja

Utrzymywanie komunikacji z klientem pozwala zespołom prowadzącym testy penetracyjne na bieżąco kontrolować, czy pozostają oni w wyznaczonym zakresie testów, czy spełniają oczekiwania klienta i czy nie naruszają wyznaczonych ograniczeń. Dzięki niej mogą oni reagować na nagły wzrost zapotrzebowania klienta na zasoby jego systemu informatycznego i dostosowywać do takich zmian terminarz swoich działań. Komunikacja umożliwia im także szybie reagowanie na pojawiające się problemy spowodowane testami, oraz na potwierdzanie autentyczności i istotności znalezionych problemów. W związku z tym istotne jest określenie przez rozpoczęciem testów penetracyjnych ustalenie z klientem ścieżek komunikacyjnych.

Komunikacja

Ścieżki komunikacyjne

Zwykle, w trakcie trwania testów penetracyjnych komunikację ogranicza się do trzech osób:

podstawowy kontakt (ang. *primary contact*) osoba odpowiedzialna za codzienne administrowanie sprawami związanymi z testami penetracyjnymi;

kontakt techniczny (ang. *technical contact*) osoba zajmująca się kwestiami technicznymi lub udzielająca odpowiedzi na pytania techniczne, które mogą się pojawić w trakcie testów;

kontak awaryjny (ang. *emergency contact*) zespół, taki jak SOC (ang. *Security Operations Center*), dostępny przez 24h/dobę, który odpowiedzialny jest za reagowanie na incydenty.

Zespół testujący powinien również regularnie informować, w ramach krótkich spotkań, osoby zainteresowane (ang. *stakeholders*) po stronie klienta o postępach testów i wyjątkowych kwestiach. Częstość tych zebrań zależy od szacowanego czasu trwania testowania penetracyjnego.

Komunikacja

Zdarzenia

Oprócz ścieżek komunikacji i regularnych spotkań należy także ustalić z klientem listę wyjątkowych zdarzeń, będących powodem do nawiązania wymiany informacji poza przyjętymi ustaleniami. Takim zdarzeniami zazwyczaj są:

zakończenie etapu testów testowanie penetracyjne, tak jak inne rodzaje testowania, powinno być podzielone na etapy, a o ich zakończeniu powinni być informowani klienci;

odkrycie krytycznej podatności krytyczne luki bezpieczeństwa narażają na zbyt duże ryzyko zasoby informatyczne zleceniodawców, zatem powinny być przez testerów natychmiast raportowane, nawet gdyby ich załatanie miało utrudnić dalsze testy lub uniemożliwić osiągnięcie ich zamierzonego celu;

odkrycie śladów włamania o znalezieniu dowodów zakończonego lub trwającego prawdziwego ataku testerzy powinni niezwłocznie poinformować klientów.

Komunikacja

Zmiana priorytetów

Nawet najstaranniej przygotowane plany testów penetracyjnych mogą ulec zmianie w trakcie ich realizacji, dlatego niezbędne jest opracowanie procedur na taką okoliczność. Jeśli te zmiany są znaczące i wychodzą poza uzgodniony zakres prac, to należy je skonsultować ze wszystkimi zainteresowanymi stronami. W przypadku mniej znaczących modyfikacji może to nie być konieczne, ale może być pomocne.
Wszystkie kwestie dotyczące komunikacji powinny być ujęte w zakresie prac (ang. *statement of work*).

Raport

Raport stanowi podsumowanie głównych prac związanych z testami penetracyjnymi. Nie ma ustalonego formatu raportu, ale istnieją wytyczne, związane np. ze standardami PCI SSC. Typowo raport powinien zawierać:

- podsumowanie dla kierownictwa,
- szczegóły zakresu,
- opis metodologii,
- odkrycia i zalecenia,
- wnioski,
- dodatki.

Raport

Podsumowanie dla kierownictwa

Podsumowanie dla kierownictwa jest prawdopodobnie najważniejszą częścią raportu, a jej sporządzenie wymaga od zespołu testerów posiadania osób o „miękkich umiejętnościach”. Odbiorcami tej części są bowiem osoby, które niekoniecznie posiadają wiedzę na temat cyberbezpieczeństwa, czy nawet informatyki. Mają one jednak uprawnienia decyzyjne w firmie, instytucji lub organizacji zlecającej testy. Dlatego też od tego rozdziału zależą dalsze czynności związane z usuwaniem podatności i ich skuteczność. Należy zatem w tej części raportu zwięźle i bez szczegółów technicznych przestawić znalezione luki zabezpieczeń i opisać, w sposób nieprzesadzony, związane z nimi ryzyko. Zwięzłość w tym wypadku niekoniecznie oznacza jedną stronę, ale ogółem małą liczbę stron. Choć opisywany rozdział powinien się znaleźć jako pierwszy w raporcie, to warto jego opracowanie pozostawić na koniec.

Raport

Szczegóły zakresu

W tej części należy opisać planowany zakres testów oraz wszelkie jego zmiany, jakie zaszły w ich trakcie. Te informacje nie tylko zamieszcza się w raporcie ze względów kronikarskich, ale również aby nadać kontekst pozostałym rozdziałom oraz wskazać co było, a *co nie było* celem i przedmiotem testów. Może to być także istotne przy ewentualnych reklamacjach i zastrzeżeniach ze strony klienta.

Raport

Metodologia

Ten rozdział raportu jest skierowany do osób posiadających odpowiednią wiedzę techniczną i zajmującymi się po stronie klienta bezpieczeństwem systemów informatycznych. To tutaj powinny znaleźć się wszystkie niezbędne techniczne szczegóły. Należy wyjaśnić, które rodzaje testów zostały przeprowadzone, przy użyciu jakich narzędzi i jakie poczyniono obserwacje. Osoba czytająca tę część sprawozdania, zakładając że dysponuje odpowiednią wiedzą w zakresie cyberbezpieczeństwa, powinna być w stanie powtórzyć przedstawione testy i otrzymać takie same wyniki.
Przedstawione detale testowania powinny przekonać czytelnika o dobrej jakości pracy wykonanej przez testerów i umożliwić mu zrozumienie ich sposobu działania. Z drugiej strony zamieszczanie w tej części obszernych listingów, rezultatów skanowania i innych wymagających żmudnej analizy wyników nie jest dobrym pomysłem. Lepiej umieścić je w dodatku/dodatkach.

Raport

Odkrycia i zalecenia

W tej części zamieszcza się opisy odkrytych podatności, sposobów ich reprodukcji i zalecenia odnośnie ich naprawy. Każdy opis luki powinien także zawierać informację o ryzyku z nią związanym, w szczególności:

- ocenę ryzyka, wyliczoną np. z uzyciem kalkulatora CVSS;
- priorytet zagrożenia, bazujący na jego prawdopodobieństwie i wpływie na aktywa systemu informatycznego;
- analizę wpływu na działalność firmy, instytucji lub organizacji.

Raport

Odkrycia i zalecenia

Proponowane środki zapobiegawcze mogą należeć do jednej z czterech kategorii:

środki techniczne obejmują wzmacnianie zabezpieczeń systemu (ang. *system hardening*), walidację danych wejściowych, filtrowanie poczty, wieloskładnikowe uwierzytelnienie, itp.;

środki administracyjne oznaczają wdrożeniem procesów mających na celu poprawę bezpieczeństwa, takich jak system kontroli dostępu bazując na rolach, wprowadzenie bezpiecznego cyklu tworzenia oprogramowania, itp.;

środki operacyjne to procedury mające na celu poprawę bezpieczeństwa personelu, takie jak rotacja stanowisk, ograniczenie czasu logowania, obowiązkowe urlopy, szkolenia.

środki fizyczne mają zapobiec uzyskaniu przez intruzów fizycznego dostępu do systemów informatycznych i obejmują westybule bezpieczeństwa, monitoring, zabezpieczenia biometryczne.

Raport

Odkrycia i zalecenia

Często spotykaną podatnością są konta administratorskie w systemie, które są współdzielone przez kilka osób. Umożliwia to tym osobom wyparcie się działań, które mogą stanowić zagrożenie, co jest także możliwe w przypadku współdzielonych zwykłych kont użytkowników. Problem ten można rozwiązać np. przez użycie narzędzi umożliwiających czasowe uzyskanie uprawnień administratora zaufanym użytkownikom (np. polecenie `sudo` w Linuksie), lub zastosowanie odpowiedniego managera haseł lub dostępu (np. narzędzie *Local Administrator Password Solution* — LAPS firmy Microsoft). W przypadku drugiej opcji należy stosować skomplikowane hasło, które będzie udostępniane tylko zaufanym użytkownikom i tylko w nagłych przypadkach. Najlepiej, żeby Ci użytkownicy nie mogli poznać tego hasła oraz żeby było ono zmieniane po jednorazowym użyciu.

Raport

Odkrycia i zalecenia

Innym często spotykanym problemem jest mała złożoność haseł (ang. *weak password complexity*). To zagrożenie można zniwelować stosując odpowiednią politykę haseł, co jest możliwe zarówno w systemie operacyjnym ▸ Windows, jak i ▸ Linux oraz w oprogramowaniu użytkowym. Należy jednak pamiętać, aby nie przesadzić ze złożonością hasła, ani częstotliwością jego zmiany. Badania psychologiczne udowodniły, że ludzie zmuszeni do częstej zmiany haseł tworzą je podobne, posługując się prostymi schematami. Zamiast stosować skomplikowane hasła lepiej wdrożyć inne mechanizmy uwierzytelniające.

Raport

Odkrycia i zalecenia

Rozwiązaniem części problemów z hasłami może być wdrożeniem *wieloskładnikowego uwierzytelniania* (ang. *multifactor authentication*), które sprowadza się do potwierdzania tożsamości użytkownika z użyciem dwóch składników, należących do poniższych kategorii:

To co wiesz do tej kategorii należą hasła i PINy, czyli tajne informacje znane tylko użytkownikowi.

Coś co masz najczęściej token sprzętowy lub programowy, który generuje jednorazowe hasła, których ważność jest dodatkowo ograniczona czasowo,

To Kim jesteś do tej kategorii należą rozwiązania biometryczne.

Ostatnio rozważa się dodanie nowej kategorii **To gdzie jesteś**, czyli położenia geograficznego logującego się użytkownika. Należy podkreślić, że logowanie wieloskładnikowe wymaga użycia co najmniej dwóch mechanizmów, **należących do różnych kategorii**.

Raport

Odkrycia i zalecenia

Warto również zaznaczyć, że każdy z tych mechanizmów z osobne ma określone wady. W przypadku tokenów jest to trwałość, możliwość zgubienia lub rozsynchronizowania. Mechanizmy biometryczne bazują najczęściej na statystyce, więc zdarzają się w ich przypadku błędne rozpoznania (ang. *false positive*). Problemem mogą okazać się także choroby lub skutki wypadków użytkowników. Wśród tych systemów największą skuteczność mają skanery siatkówki, ale mogą być one podatne na ataki z użyciem fotografii lub nagrań w wysokiej rozdzielczości. Dlatego w uwierzytelnianiu wieloskładnikowym stosuje się kombinację kilku takich mechanizmów.

Raport

Odkrycia i zalecenia

Często w badanych systemach testerzy odnajdują otwarte usługi, których tam być nie powinno. Mogą one być instalowane domyślnie, wraz np. z systemem operacyjnym lub zostały świadomie uruchomione przez administratorów w określonym celu, ale po jego osiągnięciu nie zostały wyłączone. Takie usługi mogą być problematyczne, ponieważ świadczące je oprogramowanie może nie być aktualizowane lub nawet poprawnie skonfigurowane.
Środkiem zapobiegającym powstawaniu takiego problemu jest wzmacnianie zabezpieczeń systemu. Należy je przeprowadzić zaraz po jego początkowej konfiguracji, a następnie powtarzać okresowo, dostosowując konfigurację systemu do bieżących potrzeb użytkującej go firmy, instytucji lub organizacji.

Raport

Wnioski

Ta cześć raportu powinna podsumowywać wyniki testów penetracyjnych i zawierać zalecenia odnośnie do przyszłych działań, np. poszerzenie zakresu testów. Wnioski mogą również zawierać metryki oceniające globalnie ryzyko związane z wykrytymi lukami bezpieczeństwa i porównujące je do poziomu tolerancji ryzyka deklarowanego przez zlecający podmiot. Można także wskazać w tym rozdziale najbardziej priorytetowe działania, jakie należy wykonać oraz główne przyczyny problemów z bezpieczeństwem w danej firmie, instytucji lub organizacji, o ile uda się je zidentyfikować.

Raport

Dodatki

Tworzenie dodatków w raporcie nie jest konieczne. Jeśli jednak testerzy dojdą do wniosku, że obszerne kody źródłowe, wyniki skanowania lub wymagające wnikliwej analizy wyniki mogą być dla czytelnika pomocne, to powinni je umieścić w dodatkach, a w innych częściach raportu zamieścić do nich odwołania.

Raport

Przekazanie raportu

Raport z testów penetracyjnych zazwyczaj jest klasyfikowany jako *tajny* lub co najmniej *poufny*, bo zawiera informacje, których przejęcie przez nieuprawnione osoby może narazić klienta na poważne problemy. Zatem na etapie planowania testowania penetracyjnego należy określić kto, personalnie, będzie uprawniony do odbioru takiego dokumentu, w jaki sposób ten raport powinien zostać zaszyfrowany oraz jak powinny być przechowywane jego kopie papierowe. Umowa między testerami, a klientem może określać po jakim czasie i w jaki sposób testerzy powinni zniszczyć posiadane kopie raportu, wraz z notatkami sporządzonymi podczas testów i ich innymi wynikami.

Firma *Securitum* udostępnia, za zgodą klientów dwa raporty z testów bezpieczeństwa. Informacje w nich zawarte uległy już przedawnieniu i nie ich ujawnienie nie stanowi zagrożenia. Pierwszy z nich został przygotowany dla firmy ▸ YetiForce, a drugi na zlecenie bliżej nieokreślone, a drugi na zlecenie bliżej nieokreślonej ▸ firmy medycznej.

Czynności końcowe

Sprzątanie systemu

Przekazanie raportu nie kończy prac związanych z testami penetracyjnymi. Jest kilka ważnych czynności które należy wykonać. Pierwszą z nich jest usunięcie z systemu wszelkich narzędzi i zmian konfiguracji, które powstały w trakcie jego testowania. W szczególności należy:

- usunąć odwrócone i wiązane powłoki,
- konta założone podczas testów i zainstalowane tylne furtki,
- inne narzędzie pozostawione w systemie.

W tej czynności pomaga dokumentowanie w trakcie testów dokonywanych zmian. Jedynymi modyfikacjami, które nie muszą, a nawet nie powinny być usuwane, są te, które mają na celu naprawienie znalezionych krytycznych podatności.

Czynności końcowe

Ponowne testy

Klient może poprosić o wykonanie dodatkowych testów, np. przy użyciu innych narzędzi lub dotyczących innych celów. Jeśli te prace nie wykraczają poza zakres poprzedniego testowania, to mogą one być zrealizowane od razu, w ramach tej samej umowy. Jeśli jednak wymagałby one znaczącej zmiany zakresu, to powinny być przedmiotem osobnych negocjacji, a później przygotowań. Zamawiający podmiot może także poprosić o powtórne testy (ang. *retests*), po usunięciu wskazanych przez testerów istotnych podatności. Należy te testy przeprowadzić nie później niż 6 miesięcy od usunięcia wspomnianych luk, bo później zmiany w systemie mogą być na tyle duże, że trudno będzie ocenić, czy są w nim nowe podatności, czy poprzednio odkryte nie zostały skutecznie naprawione. Powtórne testy mogą być przedmiotem osobnej umowy z klientem.

Czynności końcowe

Retrospekcja

Po zakończonych testach zespół powinien ponownie się zgromadzić i przedyskutować przebieg procesu testowania. Dobrą praktyką jest zaproszenie kogoś z zewnątrz zespołu w roli moderatora tej dyskusji. Jej przedmiotem powinna być analiza napotkanych problemów i zidentyfikowanie działań i metod, które dały korzystne wyniki i być może warto będzie je wdrożyć w przyszłych zleceniach.

Czynności końcowe

Odbiór i inne zagadnienia

Z punktu widzenia zespołu testerskiego najważniejszy jest odbiór przez klienta wyników testów penetracyjnych, potwierdzony formalnym dokumentem. Jeśli te testy zostały przeprowadzone, aby spełnić wymogi określonego standardu, to klient może także oczekiwać formalnego oświadczenia, że te wymagania są przez jego system informatyczny spełniane. W takich przypadkach warto przez rozpoczęciem testów i podpisaniem umowy z klientem upewnić się, że czy ten standard wymaga posiadania przez członków zespołu testującego odpowiednich certyfikatów, a jeśli tak, to czy w zespole są osoby z takimi certyfikatami. Testerzy powinni także skrupulatnie przestrzegać zapisów umowy z klientem regulujących kwestię przechowywania i niszczenia danych uzyskanych w trakcie testowania jego systemu.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!