Testy Penetracyjne

Planowanie i określanie zakresu

Arkadiusz Chrobot

Katedra Systemów Informatycznych

6 marca 2024

Plan

Wstęp

Jednym z elementów odróżniających testy penetracyjne od rzeczywistych ataków przeprowadzanych przez intruzów jest faza formalnego planowania. Jej przebieg jest zależny od założonego celu testów penetracyjnych, zespołu, który będzie je przeprowadzał (wewnętrzny lub zewnętrzny) oraz typu potencjalnych agresorów. W trakcie planowania określa się ramy czasowe testów, ich zakres (elementy systemu informatycznego, których bezpieczeństwo powinno być zweryfikowane) oraz przebieg.

Zasady zatrudnienia

Zasady zatrudnienia (ang. *Rules of Engagement* — *RoE*) w przypadku testów penetracyjnych obejmują:

- ramy czasowe testów, w szczególności kiedy mogą być one przeprowadzone,
- które systemy, lokalizacje i inne potencjalne cele są w zakresie testów,
- typy testów, które są dozwolone lub zabronione,
- sposób postępowania z informacją zgromadzoną podczas testów,
- spodziewanego zachowania celów,
- zasobów udostępnionych testerom,
- kwestie prawne,
- komunikację z klientem,
- osobę kontaktową, w przypadku wystąpienia szczególnych okoliczności,
- podmiot/osobę zatrudniającą.

Zasady zatrudnienia

Ramy czasowe testów

Ramy czasowe testów penetracyjnych mogą określać nie tylko ile dni, czy nawet miesięcy zajmie testowanie, ale również w których dniach, a nawet godzinach powinno być przeprowadzone. Jeśli testy mogą negatywnie wpłynąć na działanie usług systemów informatycznych, które niezbędne do prowadzenia działalność klienta, to może on wymagać, aby były one przeprowadzone poza normalnymi godzinami pracy. Jeżeli natomiast ich celem jest ocena reakcji zespołów reagowania na ataki cybernetyczne pracujących dla klienta, to powinny być wykonane w godzinach pracy.

Zasady zatrudnienia

Dozwolone i niedozwolone typy testów

Najczęściej wykluczanymi typami testów penetracyjnych są te mogące mieć destruktywny wpływ na oceniane systemy, ale również testy socjotechniczne lub zabezpieczeń fizycznych (drzwi, pomieszczeń, itd.). Jednak w niektórych przypadkach klient może zgodzić się na ich przeprowadzenie lub wręcz na to nalegać. Dlatego na etapie planowania należy dokładnie określić jakie metody testowania mogą być zastosowane.

Zasady zatrudnienia

Sposób postępowania z uzyskanymi informacjami

Te zasady są szczególnie ważne w przypadku systemów informatycznych przechowujących dane medyczne lub mające znaczenie dla obronności lub funkcjonowania kraju, ale również mają zastosowanie dla „zwykłych” danych osobowych. Mogą określać nie tylko okres przechowywania tych informacji (ang. *data retention*), ale również sposób ich przekazania przedstawicielom klienta, metodę ich usunięcia (ang. *disposal*), a także to czy i w jaki sposób powinny być te dane szyfrowane w trakcie i po zakończeniu testów.

Zasady zatrudnienia

Zachowanie celu

Należy określić czy i jakie działania defensywne może podjąć atakowany podmiot w trakcie testów penetracyjnych. Jeśli mają one ocenić całościowo zabezpieczenia jego infrastruktury informatycznej, to blokowanie ruchu sieciowego, aktualizacja reguł zapór sieciowych i inne czynności mogą to zadanie utrudnić. Natomiast w przypadku weryfikacji zdolności obronnych takie operacje są jak najbardziej dozwolone.

Zasady zatrudnienia

Jakie zasoby zostaną udostępnione testerom

Rodzaj zasobów, które klient udostępni zespołowi przeprowadzającemu testy penetracyjne zależy od tego, czy będą to testy znanego środowiska, nieznanego, czy pośrednie. Największe restrykcje pod tym względem występują w drugim z wymienionych przypadków. Jeśli testy dotyczyć mają znanego lub częściowo znanego środowiska, to testerzy mogą uzyskać całkowity lub częściowy dostęp do dokumentacji weryfikowanego systemu, takiej jak wewnętrzna baza wiedzy, diagramy architektury systemu, pliki konfiguracyjne, dokumentacja API, narzędzia SDK, lub dokumentacja narzędzi dostarczanych przez podmioty zewnętrzne (ang. *third-party*).
Testerzy mogą otrzymać nie tylko dostęp do kont nieuprzywilejowanych i uprzywilejowanych użytkowników, ale również mogą liczyć na dodanie ich działań do listy wyjątków w mechanizmach bezpieczeństwa typu WAF, IDS, a także na dostęp fizyczny do elementów infrastruktury.

Zasady zatrudnienia

Kwestie prawne

Systemy informatyczne podlegające testom penetracyjnym mogą być rozległe również pod względem geograficznym, zatem poszczególne ich elementy mogą podlegać różnym jurysdykcjom. W takim przypadku konieczne jest określenie jakie działania i jakie narzędzia mogą być zastosowane w przeprowadzanych na nich testach. Na przebieg testów penetracyjnych może mieć także prawo dotyczące systemów informatycznych specjalnego przeznaczenia.

Zasady zatrudnienia

Komunikacja z klientem

Przed rozpoczęciem testów należy ustalić jak często wykonawca ma kontaktować się z klientem. Czy ma informować o postępach prac każdego dnia, tygodnia, czy też po prostu złożyć raport końcowy po ukończeniu testowania?

Zasady zatrudnienia

Postępowanie w sytuacjach wyjątkowych

Testy penetracyjne nie zawsze przebiegają bezproblemowo, więc wykonawca i klient powinni ustalić reguły postępowania w razie wystąpienia problemów, takich jak np. odkrycie rzeczywistego ataku w trakcie jego realizacji, lub po zakończeniu, odkrycie krytycznej podatności, ▸ przypadkowe złamanie reguł zatrudnienia lub poważne zakłócenie działania badanego systemu informatycznego. W tym ostatnim przypadku pomocne jest dokumentowanie czynności wykonywanych przez pentesterów (testerów penetracyjnych). Ułatwi to współpracę z zespołem reagowania klienta, odtworzenie działań i wykrycie rzeczywistych przyczyn awarii.

Zasady zatrudnienia

W zasadzie pierwszą kwestią, którą powinna ustalić firma, dla której pracują pentesterzy, to przedstawiciel lub przedstawiciele klienta, którzy są **rzeczywiście** upoważnieni do zatrudniania zespołów testujących, aby uniknąć ▸ poważnych kłopotów.

Zakres

Zakres testów penetracyjnych powinien określać nie tylko co podlega testom, ale szczególnie to co im **nie podlega**. Umowa z klientem powinna zawierać oświadczenie, że wyniki testów są ważne (ang. *valid*) tylko w czasie, kiedy te testy zostały przeprowadzone, a na ich jakość ma wpływ przyjęta metoda testowania i zdefiniowany zakres. Ustalenie zakresu testów jest szczególnie trudne w przypadku weryfikacji nieznanego środowiska, ale nawet w testach znanego i częściowo znanego środowiska może wystąpić ten problem, jeśli nie istnieje dokładna dokumentacja weryfikowanego systemu. Dodatkowo, nawet przy precyzyjnym określeniu zakresu, w trakcie testów może pojawić się przeszkoda uniemożliwiająca osiągnięcie założonego celu. W takim wypadku może się okazać, że konieczne będzie np. nieplanowane wyłączenia przez pentestera określonego mechanizmu zabezpieczającego, celem rozwiązania tego problemu.

Zakres

Odrębnym zagadnieniem jest powiązanie testowanego systemu informatycznego z innymi systemami, np. typu chmurowego. Właściciele takich systemów zazwyczaj nie pozwalają przeprowadzać na nich testów penetracyjnych klientom. Należy więc je wyłączyć z weryfikacji lub uzyskać zgodę na testowanie.
Trzeba także mieć na uwadze poziom ryzyka jaki jest w stanie zaakceptować klient w związku z prowadzeniem testów penetracyjnych. To pomoże ustalić, czy np. elementy systemu o znaczeniu krytycznym mają być przedmiotem weryfikacji.
W końcu należy też uwzględnić ograniczenia czasowe i budżetowe. Zakres nie może być większy niż pozwala na to czas i koszty testowania penetracyjnego. W szczególności należy unikać nadmiernej rozbudowy zakresu (ang. *scope creep*).

Zakres

Przykłady pytań pozwalających ustalić zakres testów penetracyjnych WAN/LAN

1. Ile adresów IP lub jaka maska sieciowa podlega weryfikacji?
2. Ile w przybliżeniu urządzeń jest podłączonych do sieci?
3. Ile lokalizacji fizycznych obejmuje sieć LAN?
4. Czy testy tych urządzeń mogą być przeprowadzone zdalnie?
5. Czy weryfikacja może w całości być przeprowadzona tylko z jednego urządzenia?
6. Czy weryfikacja może w całości być przeprowadzona tylko z jednego miejsca?
7. W jakich porach można przeprowadzić test?
8. Czy wymagane będą ponowne testy?

Standardy i metodologie

Zdefiniowanie od podstaw scenariusza, według którego ma przebiegać konkretny test penetracyjny, jest trudne. Dlatego powstały standardy i poradniki, które ułatwiają to zadanie. Należą do nich:

The MITRE ATT&CK Framework jest to ▸ baza wiedzy na temat znanych taktyk i technik ataków stosowanych przez intruzów. Sama w sobie nie jest standardem lub planem testów penetracyjnych, ale może posłużyć do ich budowy, szczególnie w aspekcie technicznym.

Penetration Testing Execution Standard (PTES) choć ten dokument pochodzi z 2014 roku, to nadal jest aktualny i opisuje rekomendowany przebieg poszczególnych faz testu penetracyjnego.

Standardy i metodologie

Open Source Security Testing Methodology Manual (OSSTMM) jest jeszcze starszym dokumentem niż PTES — pochodzi z 2010 roku — ale jest też bardziej obszerny, zawiera opisy metryk, sposobów analizy systemów, bezpieczeństwa sieci bezprzewodowych, itd. Z uwagi na datę wydania może nie zawierać opisów najnowszych technik ataków.

Information Systems Security Assesment Framework (ISSAF) to opracowany w 2005 roku standard autorstwa *Open Information Systems Security Group* (OSSIG) — wersja, do której prowadzi łącze jest jeszcze starszym szkicem, ponieważ wersja ostateczna nie jest obecnie dostępna — to szczegółowy (około 1200 stron) standard testów penetracyjnych, który niestety nie jest już całkiem aktualny.

Standardy i metodologie

NIST Technical Guide to Information Security Testing and Assessment to formalny dokument standaryzujący między innymi testy penetracyjne. Choć był on aktualizowany ostatnio w 2008 roku, to zgodność z nim może być wymagana przez niektóre instytucje, szczególnie związane z USA.

OWASP Application Security Verification Standard bardzo rozbudowany i w miarę aktualny (wersja 4.0 wydana w marcu 2019), standard bezpieczeństwa dla aplikacji webowych. Istnieje także jego odpowiednik dla aplikacji mobilnych z 2024 roku. Spełnienie wszystkich opisanych w tych standardach wymagań wydaje się niemożliwe, ale są one dobrym punktem startowym, do określenia przebiegu testów penetracyjnych.

Umowy i inne dokumenty

Etap planowania i określania zakresu testów penetracyjnych powinien się zakończyć uzyskaniem i/lub podpisaniem szeregu dokumentów, do których mogą się zaliczać:

Główną umowę o świadczeniu usług (ang. *Master Service Agreement*), to dokument, który określa warunki długoterminowej współpracy między zespołem pentesterów, a klientem.

Zakres prac (ang. *Statement of Work*) określa cel konkretnych testów penetracyjnych, definiuje jakie czynności w ich ramach będą wykonane i jakich rezultatów spodziewa się klient, a także czas ich przeprowadzenia i wynagrodzenie pentesterów. Może odwoływać się do głównej umowy o świadczeniu usługi, jeśli została ona wcześniej podpisana.

Umowy i inne dokumenty

Umowę o nieujawnianiu lub poufności (ang. *Nondisclosure Agreement*, NDA) lub (ang. *Confidentiality Agreement*, CA), to osobne umowy zobowiązujące wykonawców testów penetracyjnych do zachowania poufności, w szczególności do nieujawniania poufnych informacji uzyskanych w wyniku prowadzenia weryfikacji.

Umowa o poziomie usług (ang. *Service Level Agreement*, SLA) tego typu umowy podpisywane są zazwyczaj między dostawcami usług, a ich odbiorcami, ale mogą one być przedmiotem zainteresowania pentesterów, lub zespoły testujące będą musiały się zobowiązać, że nie naruszą takich umów, które zawarł klient ze stronami trzecimi.

Umowa o niekonkurowaniu (ang. *Non-compete Agreement*) może być podpisana między pentesterem, a jego pracodawcą i zakazywać mu przejścia do konkurencyjnej firmy. Ma zazwyczaj charakter czasowy.

Umowy i inne dokumenty

Oprócz umów, dla testów penetracyjnych są lub mogą być istotne następujące dokumenty:

Pozwolenie na atak (ang. *Permission to Attack* (*Authorization*)) formalna zgoda klienta na przeprowadzenie testów penetracyjnych należących do niego systemów informatycznych.

Zgoda stron trzecich (ang. *Third-Party Authorization*) formalna zgoda innych podmiotów, które współpracują z klientem i na których systemy informatyczne mogą mieć wpływ prowadzone testy.

Kwestie własności i przechowywania (ang. *retention*) danych uzyskanych w trakcie testów penetracyjnych mogą być regulowane osobnymi dokumentami.

Zgodność z regulacjami

W ramach testów penetracyjnych testerzy mogą być poproszeni o sprawdzenie zgodności zabezpieczeń badanego systemu informatycznego ze regulacjami prawnymi lub obowiązującymi w danej branży. Najczęściej może chodzić o zgodność z GDPR/RODO lub PCI DSS, ale także NIST FIPS 140-2, HIPAA lub dokumentami publikowanymi przez ENISA. Wykonawcy mogą się podjąć takiej oceny, o ile jest to w zakresie ich kompetencji i mają do tego odpowiednie uprawnienia.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!