Helion

Strategie Red Team

Ofensywne testowanie zabezpieczeń w praktyce

Johann Rehberger

Tytuł oryginału: Cybersecurity Attacks - Red Team Strategies: A practical guide to building a penetration testing program having homefie

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-7404-1

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/stofte
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Część II. Taktyki i techniki 163

Rozdział 5. Świadomość sytuacyjna — mapowanie własnego terytorium za pomocą grafowych baz danych 165

Rozdział 6. Budowanie kompleksowego grafu wiedzy 187

ROZDZIAŁ 1

Uruchamianie programu bezpieczeństwa ofensywnego

Może się wydawać, że w porównaniu ze zwykłym zhakowaniem zasobów organizacji opracowanie programu ofensywnego bezpieczeństwa w jej ramach to duże wyzwanie, ale jest to jedno z najbardziej ekscytujących zadań, jakie może wykonać pentester, kierownik lub menedżer. Uczestniczenie w aktywnym projektowaniu strategii zmiany kultury bezpieczeństwa całej organizacji to świetna szansa rozwoju, a także satysfakcjonująca i przyjemna praca.

Dla kierownika i menedżera zespołu ofensywnego bezpieczeństwa niezwykle ważne jest ustalenie jasnych zasad oraz nakreślenie wizji i reguł dla zespołu. Omawiam tu aspekty, które należy uwzględnić w tym procesie, i prezentuję kilka pomysłów dotyczących tego, jak zbudować trwałe fundamenty.

W tym rozdziale omówione zostaną następujące tematy:

- definiowanie praktycznej misji dla cyberoperacyjnego programu zespołu czerwonego,
- znalezienie poparcia wśród wpływowego kierownictwa w celu ustanowienia programu czerwonego zespołu,
- strategie określające miejsce zespołu czerwonego w organizacji,
- znaczenie tworzenia harmonogramu bezpieczeństwa ofensywnego,
- zrozumienie wyjątkowych umiejętności wymaganych na tym stanowisku, a także sposobów przyciągania i zatrzymywania inżynierów i myślicieli z drugiej strony barykady,

- oferowanie organizacji różnych usług zespołu czerwonego,
- ustalanie zasad, reguł i standardowych procedur operacyjnych mających na celu dojrzewanie programu,
- modelowanie przeciwnika i zrozumienie anatomii włamania,
- rozważania na temat otwartych i zamkniętych przestrzeni biurowych oraz ich wpływu na bezpieczeństwo i kulturę zespołu.

Definiowanie misji — adwokat diabła

Ogólnie rzecz biorąc, czerwony zespół najlepiej potraktować jak adwokata diabła. Taka wizja ma zagwarantować rozważenie alternatywnych poglądów i uwzględnienie zainteresowanych stron. Celem programu ofensywnego bezpieczeństwa jest sprowadzanie ludzi na ziemię w czasie formowania konsensusu. Odbywa się to poprzez wykazanie nie tylko teoretycznego, ale także rzeczywistego wpływu wykorzystania słabych punktów oraz przedstawienie tego osobom odpowiedzialnym w organizacji za zarządzanie ryzykiem.

Pod wieloma względami program ofensywny spełnia w organizacji funkcję testowania bezpieczeństwa — funkcję czasami rzadką, ale jednak bardzo potrzebną we współczesnym świecie inżynierii oprogramowania, poruszania się po wszystkich warstwach stosu technologicznego (ang. *full-stack development*) i DevOps.

Aby uruchomić skuteczny wewnętrzny program bezpieczeństwa ofensywnego, ważna jest prosta, ale inspirująca misja, która ma pomóc w prezentowaniu celu i motywowaniu zespołu. Misja powinna dotyczyć tego, jakie działania mają być podejmowane — nie ma powodu zagłębiania się w to, jak mają być osiągane. Dobrym punktem wyjścia może być misja polegająca na naśladowaniu wrogich zachowań oraz znajdowaniu i wykorzystywaniu luk w zabezpieczeniach w celach obronnych.

Podkreślenie aspektu defensywnego jest ważne, ponieważ celem dojrzałego czerwonego zespołu powinna być poprawa nastawienia do kwestii bezpieczeństwa w organizacji i napędzanie zmian kulturowych. Głównym celem zespołu czerwonego jest pomoc organizacji w zrozumieniu jej słabych punktów, wskazanie ich oraz pomoc we wprowadzaniu usprawnień i mierzeniu efektywności tych usprawnień z biegiem czasu. Samo znalezienie i zbadanie problemu nie prowadzi automatycznie do zmiany. To pierwsza wielka przeszkoda na drodze wprowadzania programu ofensywnego, który ma na celu ulepszenie organizacji. Aby osiągnąć zmianę kulturową i poprawić stan bezpieczeństwa organizacji, czerwony zespół potrzebuje jakiejś formy pomiaru i sposobu prezentowania kluczowych wskaźników efektywności (ang. *key performance indicator* — KPI) organizacji i kierownictwu, aby można było świadomie inwestować. Pomysły dotyczące metod realizowania tych celów omówię w rozdziale 3., „Mierzenie efektywności programu bezpieczeństwa ofensywnego”.

Jak już wspominałem, ważnym aspektem zespołu ofensywnego bezpieczeństwa jest napędzanie zmiany kulturowej, więc dobrym pomysłem jest również uwzględnienie w celu misji poprawy postawy dotyczącej kwestii bezpieczeństwa i kultury bezpieczeństwa organizacji.

Oto kilka wskazówek dotyczących formułowania celu misji:

- bycie adwokatem diabła,
- naśladowanie działań przeciwników w celach obronnych,
- mierzenie, prezentowanie i poprawianie bezpieczeństwa organizacji,
- zwiększenie IQ bezpieczeństwa organizacji,
- łamanie norm i rzucanie wyzwań efektywności organizacji,
- dostarczanie alternatywnych analiz i „myślenie kategoriami przeciwnika",
- rzucanie wyzwania wszystkiemu!

Dobrą taktyką, która może zyskać przychylność kadry kierowniczej i zarządzającej, jest odzwierciedlenie w deklaracji misji również podstawowych wartości organizacji.

Uzyskanie poparcia kadry kierowniczej

Aby z powodzeniem uruchomić program czerwonego zespołu, niezbędne jest pozyskanie aktywnego poparcia kadry kierowniczej.

Jedną z największych zalet programu ofensywnego bezpieczeństwa i generalnie działania czerwonego zespołu jest możliwość zapewnienia, aby wszyscy zachowywali się uczciwie. Ufać, ale kontrolować. Poparcie **kierownika ds. bezpieczeństwa** (ang. *Chief Security Officer* — CSO) jest prawdopodobnie łatwe do zdobycia, ale poparcie, o którym mowa, musi sięgać dalej. Musi obejmować również inne szczeble kierownicze organizacji. Mógłbym to powtarzać w nieskończoność: jeśli nie ma aprobaty kadry kierowniczej, skuteczność i wyniki programu będą ograniczone. Uzyskanie długoterminowego poparcia można osiągnąć, stosując różne strategie, w tym dostarczanie danych i przedstawianie liczb odzwierciedlających rzeczywiste akty naruszenia bezpieczeństwa oraz wyjaśnianie ich wpływu na organizację.

Przekonywanie kierownictwa za pomocą danych

Analizując dane, warto przyjrzeć się krajobrazowi konkurencji i przeanalizować ostatnie naruszenia bezpieczeństwa, które miały miejsce w branży, oraz powiązane z nimi wpływy, jakie wywarły na dane organizacje. Może to obejmować takie dane jak:

- zbieranie informacji związanych z kosztami i wpływem naruszeń bezpieczeństwa w branży,
- zbieranie danych dotyczących wcześniejszych naruszeń bezpieczeństwa w Twojej organizacji,

- zbieranie dowodów innych incydentów dotyczących bezpieczeństwa w Twojej organizacji,
- jeśli Twoja organizacja przechodziła w przeszłości testy penetracyjne lub testy czerwonego zespołu (np. ze względu na spełnienie określonych norm), spróbuj zdobyć wcześniejsze ustalenia i wyniki oraz przyjrzyj się ich wpływowi biznesowemu na poparcie dalszych inwestycji i zachętę do nich,
- jeśli wdrożyłeś już program nagradzania za znajdowanie luk bezpieczeństwa (ang. *bug bounty program*), jego wyniki i ustalenia mogą dodatkowo podkreślić konieczność inwestowania w tym obszarze.

Przekonywanie kierownictwa za pomocą działań i wyników

Kolejnym podejściem jest zaproponowanie lekkiego ofensywnego testu penetracyjnego (ang. *penetration test*) w celu zbadania, czy organizacji przydałoby się więcej inwestycji. Może to być proste studium przypadku, coś w rodzaju przeszukiwania intranetu i kodu źródłowego pod kątem haseł w postaci zwykłego tekstu. Następnie trzeba przeprowadzić analizę ryzyka spustoszenia, jakie mógłby spowodować złośliwy członek wewnętrznego personelu, mając wgląd w powszechnie dostępne hasła. Można to zrobić wewnętrznie lub wynająć jedną z wielu świetnych organizacji konsultingowych w celu zwrócenia uwagi na potencjalne problemy.

Miejsce czerwonego zespołu w schemacie organizacyjnym

Początkowo nie zastanawiałbym się zbytnio, jakie miejsce w organizacji powinien zajmować zespół bezpieczeństwa ofensywnego. Jeśli dopiero zaczynasz, najprawdopodobniej do wykonywania prac związanych z bezpieczeństwem ofensywnym zatrudniona zostanie tylko jedna osoba w pełnym wymiarze czasu pracy. Na tym etapie bardziej istotne jest zatwierdzenie przez kierownictwo i uzyskanie poparcia w przeprowadzaniu ofensywnych testów i prezentowaniu wyników. Na początku nacisk należy położyć na działania i demonstrowanie pozytywnego wpływu. W niektórych organizacjach taki program jest w całości outsourcowany i tylko logistyka jest prowadzona wewnętrznie, chociaż zazwyczaj zaczyna rosnąć chęć zbudowania wewnętrznego zespołu.

W typowej strukturze organizacyjnej zespół bezpieczeństwa ofensywnego zostanie prawdopodobnie umieszczony w dziale obrony i reagowania albo jako funkcja zespołu zapewniania bezpieczeństwa. Spotkałem się również z tym, że w niektórych firmach zespoły bezpieczeństwa ofensywnego były umieszczane w działach związanych z kwestiami prawnymi i zajmujących się zapewnianiem zgodności z normami branżowymi. Wiele zależy od wielkości i struktury organizacji, a także od wielkości samego zespołu bezpieczeństwa ofensywnego.

Świetnym miejscem w organizacji i osobiście moim ulubionym jest pełnienie funkcji kadrowej, która informuje kierownictwo (np. wiceprezesa, dyrektora generalnego lub dyrektora ds. bezpieczeństwa informacji) jako niezależna grupa. Gwarantuje to dużą autonomię i zapewnia kierownictwu bezpośredni, niefiltrowany wgląd w stan bezpieczeństwa. Jednak w większości przypadków zespół zostanie zagrzebany gdzieś głęboko w schemacie organizacyjnym i nie ma w tym nic złego. Nie podoba mi się jednak, gdy zespół przeprowadzający testy penetracyjne odpowiada przed zespołem defensywnym (np. kierownikiem zespołu niebieskiego), ponieważ może to dać mylne wrażenie dotyczące jego podstawowego celu. Zespół bezpieczeństwa ofensywnego jest przeciwieństwem zespołu defensywnego — ma na celu pomoc organizacji, ale jego zachowania i działania muszą mieć zapewniony pewien poziom niezależności i swobody.

Droga ku przyszłości bezpieczeństwa ofensywnego

W skutecznym zarządzaniu programem bezpieczeństwa ofensywnego niezwykle ważne jest zdefiniowanie ogólnego harmonogramu, który będzie stanowić podstawę działania i wskazówki na przyszłość. Mam na myśli ogólny plan na następne dwa lub trzy lata. Program najprawdopodobniej rozwinie się w sposób naturalny, jeśli początkowe inwestycje okażą się owocne, a zwrot z inwestycji będzie widoczny. Właśnie to obserwowałem w różnych organizacjach, które wdrożyły wewnętrzny program bezpieczeństwa ofensywnego. Na początku zacznij od czegoś niewielkiego, a rok lub dwa lata później rozwinie się to w prawdziwy zespół pełnoetatowych pracowników. Ogólnie rzecz biorąc, początkowo możliwe są dwie opcje. Jedną z nich jest zbudowanie programu i zespołu od podstaw, a drugą wykorzystanie już istniejących zasobów, które mogą okazać się przydatne.

Tworzenie nowego programu od podstaw

Zaczynanie od zera może się wydawać trochę przerażające, ale jest to również duża szansa dla Ciebie. W tym przypadku najbardziej prawdopodobny scenariusz zakłada, że na początku będzie to działalność jednoosobowa, a przez demonstrowanie jej wartości i wpływu biznesowego zespół zacznie rozwijać się w sposób naturalny. Może się również zdarzyć, że początkowo będziesz całkowicie polegać na specjalistycznej wiedzy zewnętrznej, aby więc wypełnić misję, będziesz musiał zatrudnić odpowiednich dostawców usług.

Dziedziczenie istniejącego programu

Jeżeli będziesz przejmować istniejący zespół lub przechodzić w firmie reorganizację, która będzie tworzyć lub konsolidować zespoły, będziesz musiał zmierzyć się z innymi unikatowymi wyzwaniami. Mam nadzieję, że jeśli chodzi o inżynierię bezpieczeństwa ofensywnego pomocnych okaże się również wiele omówionych kwestii dotyczących ludzi i zarządzania programami.

Aby wyznaczyć plan działania, trzeba najpierw zrozumieć poziom dojrzałości istniejącego już programu i zespołu. Oto kilka pytań, na które należy sobie odpowiedzieć, przejmując istniejący zespół.

- Czy procesy i dokumentacja są już wdrożone?
- Czy zdefiniowane są zasady przeprowadzania testów penetracyjnych i standardowe procedury operacyjne?
- Czy istnieją jakieś plany testowe?
- Jaka jest wielkość zespołu?
- Czy wyniki są śledzone i przeglądane?
- Czy zainteresowane strony i obowiązki są jasno zdefiniowane?

Jeżeli dopiero zaczynasz, zdefiniowanie i utworzenie niektórych z wymienionych wytycznych i reguł jest ważnym krokiem, ponieważ najprawdopodobniej Twoja organizacja nie zezwala na żadną formę ofensywnego testowania lub włamywania się do systemów. W wielu firmach za włamywanie się do innych maszyn lub uzyskiwanie dostępu do określonych zasobów możesz nawet zostać dyscyplinarnie zwolniony. Możesz przeczytać regulamin pracy swojego pracodawcy. Aby upewnić się, że wszystkie podstawy zostały omówione, w tym rozdziale opisałem kilka głównych zasad i dokumentów, które należy mieć na uwadze. Mam nadzieję, że część tych wskazówek okaże się przydatna i pomoże Ci wprowadzić testy penetracyjne w Twojej organizacji. Przed przystąpieniem do testów penetracyjnych skonsultuj wszelkie takie dokumenty i planowane działania z doradcą prawnym i innymi zainteresowanymi stronami w Twojej organizacji.

Jeśli dziedziczysz istniejący zespół, przeanalizuj model CMM (ang. *Capability Maturity Model*) dla testowania i zastanów się, jak możesz zastosować coś podobnego do testów penetracyjnych i czerwonego zespołu. Omówię to szerzej dalej w tej książce, gdy będę objaśniał mierzenie efektywności programu.

Teraz opiszę podstawy, które pomogą Ci w uruchomieniu programu i przygotowaniu podstawowego planu działania. A więc do dzieła!

Ludzie — spotkanie z członkami czerwonego zespołu

Najważniejszym elementem wdrażania udanego programu bezpieczeństwa ofensywnego jest zatrzymywanie i zatrudnianie odpowiednich ludzi, którzy mogą wypełnić jego misję. Niezależnie od tego, czy zaczynasz z tylko jednym pentesterem, czy odziedziczyłeś większy uformowany już zespół inżynierów bezpieczeństwa ofensywnego, zawsze najważniejsze są jednostki. Kształtowanie programu poprzez zatrzymywanie przy sobie i zatrudnianie właściwych ludzi ma ogromne znaczenie.

Dlaczego pentesterzy są tacy niesamowici?

Przez całą swoją karierę zawodową uważałem, że testerzy są niesamowici. Dlatego zawsze bardzo lubiłem określenie „pentester" (ang. *penetration tester*), ponieważ podkreśla ono aspekt testowania. Niestety, nie wszyscy podzielają tę opinię. Miałem przyjemność pracować i kontaktować się z jednymi z najinteligentniejszych indywidualności w dziedzinach bezpieczeństwa i bezpieczeństwa ofensywnego. Wielu z nich to zawodowi testerzy, konsultanci, badacze, inżynierowie lub pentesterzy, którzy pracowali dla dużych korporacji zatrudniających do 100 000 pracowników, a także dla mniejszych firm, ale nie brakuje wśród nich także entuzjastów bezpieczeństwa i studentów.

Jedyną rzeczą, która zawsze wyróżnia inżynierów ds. bezpieczeństwa, jest pasja, z jaką projektują swoje systemy zabezpieczeń. Często kieruje nimi idealistyczne dążenie do uczynienia świata lepszym oraz zamiłowanie do poszukiwania problemów i łamania systemów. Jeśli ktoś jest szczęśliwy, gdy może coś zepsuć, i ekscytuje go dzielenie się tą wiadomością z innymi, to znak, że prawdopodobnie jest na dobrej drodze, aby zostać pentesterem.

Mentalność „psuja" i ciekawość dotycząca wewnętrznych mechanizmów działania różnych rzeczy są bardzo potrzebne, zwłaszcza w czasach, gdy organizacje odeszły od zatrudniania specjalnych zespołów testowych. Pentester jest w tej sytuacji jak forpoczta, która pomaga organizacji zachowywać uczciwe podejście do jakości wytwarzanego produktu.

W wielu organizacjach pentesterzy są ostatnimi oddanymi swojej misji testerami, jacy jeszcze pozostali. A rezultaty ich pracy wyciągają na światło dzienne może niezbyt przyjemne, ale bardzo ważne kwestie. Ponadto są to wykwalifikowane, inteligentne, kreatywne oraz wyjątkowe osoby, z którymi zazwyczaj bardzo przyjemnie się pracuje.

Inżynieria bezpieczeństwa ofensywnego jako dyscyplina zawodowa

Niektóre organizacje nie odróżniają inżynierii oprogramowania od inżynierii bezpieczeństwa. W generalnym rozrachunku wszystko to wrzucane jest do worka ogólnie pojętej inżynierii oprogramowania, a to wielki błąd. Ważne jest podkreślenie wyjątkowości i odrębności zestawu umiejętności, jakie muszą posiadać inżynierowie ds. bezpieczeństwa, zwłaszcza pracujący na polu ofensywnym. A jaki może być najodpowiedniejszy sposób, by docenić ich wyjątkowy zestaw umiejętności? Może nadawanie im adekwatnych nazw? A nawet jeszcze lepiej — może pozwolić im wybrać własną nazwę? Adwokat diabła, inżynier bezpieczeństwa, pentester, członek czerwonego zespołu, inżynier ds. bezpieczeństwa ofensywnego, inżynier antagonistyczny, ninja bezpieczeństwa — czemuż by nie?

Ma to również związek z tym, że wynagrodzenie inżynierów bezpieczeństwa powinno być naliczane w inny sposób niż wynagrodzenie inżynierów oprogramowania i programistów. Aby dowiedzieć się, jak Twoja organizacja postrzega role inżynierów bezpieczeństwa, skontaktuj się

z działem HR. Czy istnieje jakiś znany precedens dotyczący inżynierów bezpieczeństwa ofensywnego?

Strategiczne podejście członków czerwonych zespołów

Czerwone zespoły, podobnie jak ogólnie pojęte testy penetracyjne, pełnią rolę techniczną, a czasem bardzo taktyczną. Aby się rozwijać, należy przyjąć bardziej strategiczne i analityczne cele oraz taktyki — miej to na uwadze podczas budowania zespołu. Gdy tylko osiągnięty zostanie pewien poziom dojrzałości, Twoja organizacja skorzysta na podejmowaniu działań, których nie będzie można zaszufladkować, ponieważ będą wykraczać poza przykładowe analizy infrastruktury sieciowej. Czerwony zespół przekształci się w grupę, która zawsze będzie przesuwać granice — w tym momencie poza ogólnym frameworkiem (który właściwie też powinien zostać zakwestionowany) nie ma dostępnych w tym zakresie żadnych podręczników ani poradników.

> Czerwony zespół, który nigdy nie został przetestowany i oceniony przez inny czerwony zespół, prawdopodobnie nie jest dojrzałym czerwonym zespołem.

Więcej informacji na temat dojrzewania programu bezpieczeństwa ofensywnego oraz iluzji kontroli znajdziesz dalej w tym rozdziale.

Zarządzanie programami

W zależności od wielkości zespołu czerwonego i złożoności programu sensowne może być dodanie do zespołu zasobów związanych z zarządzaniem programem. Zespół zarządzający programem może skupić się na utrzymaniu rytmu biznesowego poprzez prowadzenie regularnych spotkań informacyjnych i optymalizacyjnych. Stanie się to szczególnie przydatne, gdy program zacznie dojrzewać i konieczna będzie współpraca z innymi zainteresowanymi stronami w całej organizacji, polegająca m.in. na nadawaniu rytmu działalności, a także pomaganiu w przeprowadzaniu integracji z procesami zarządzania ryzykiem.

Przyciąganie i zatrzymywanie talentów

Wiele organizacji posiada już pewne możliwości testowania bezpieczeństwa ad hoc. Zadania te często wykonywane są przez osoby, które pracują nad modelowaniem zagrożeń i jednocześnie pomagają w praktycznych testach.

Bycie adwokatem diabła to coś, co może wydawać się wrodzone i czego nie można się nauczyć lub przekazać innym. Dobrzy pentesterzy zadają wiele pytań. Zawsze mają (czasami denerwującą) mentalność gdybania: „A co by było, gdyby…?”. To bardzo zdrowe podejście, szczególnie w przypadku ugruntowanych organizacji z długimi tradycjami *przestrzegania procedur*, które mogły zostać zoptymalizowane i zakorzeniły się w grupowym myśleniu.

Podczas rozmów kwalifikacyjnych z kandydatami na stanowiska związane z bezpieczeństwem ofensywnym przestań zadawać niepowiązane lub niepotrzebnie trudne pytania dotyczące kodowania — to nieproduktywne. Najprawdopodobniej nie szukasz inżyniera systemowego, który może opracować najszybsze i najbardziej wydajne pod względem pamięci rozwiązanie do przenoszenia poddrzew i sortowania węzłów przy jednoczesnym zachowaniu idealnej równowagi drzewa. Po prostu przestań to robić. Jeśli skupisz się właśnie na tym, nie znajdziesz osoby, której potrzebujesz.

Z pewnością warto zagłębić się w kwestie dotyczące kodowania, które pozwolą zbadać podstawowe umiejętności kandydata w tym zakresie. Niestety, z mojego doświadczenia wynika, że niektóre organizacje traktują zatrudnianie inżynierów bezpieczeństwa ofensywnego tak samo jak zatrudnianie programistów. Ty szukasz zupełnie innego zestawu umiejętności. Oczywiście, znalezienie inżyniera bezpieczeństwa, który jest jednocześnie wybitnym koderem i menedżerem programu, byłoby niesamowite, ale kiedy będziesz szukać jedynie umiejętności kodowania i stosowania algorytmów, możesz przegapić najlepszych kandydatów.

Dobre pytania powinny zawsze dotyczyć rozwiązywania problemów i „psucia" różnych rzeczy. Pozwól popsuć kandydatom coś, czego mogą nawet nie znać. Prawdopodobnie wynikiem rozmowy kwalifikacyjnej z wybitnym kandydatem będzie znalezienie nowego lub innego sposobu na popsucie czegoś.

Przed rozpoczęciem procesu rozmowy kwalifikacyjnej należy opracować spójny sposób zadawania pytań, aby można było dobrze porównywać kandydatów. Jeśli chodzi o kwestie techniczne, uznałem, że warto zadawać dwa rodzaje pytań w tym zakresie: jedno, które kandydat sam wybierze, a drugie takie, na które kandydat nie będzie znać odpowiedzi lub przyzna się do słabości w danym obszarze.

Zaufaj mi, chcesz mieć w zespole kogoś, kto *będzie w stanie przyznać się do nieznajomości czegoś*, a potem pójdzie i rozgryzie tę kwestię. Kandydat, który nie potrafi się przyznać, że czegoś nie wie, może być obciążeniem w krytycznych momentach, a zespół może zostać niemile zaskoczony, ponieważ dana osoba zmyślała, zamiast uczciwie powiedzieć, że nie zna odpowiedzi. Jesteś liderem programu i jego właścicielem. Niepowodzenie zespołu to wina lidera, a nie pojedynczego członka zespołu — zawsze o tym pamiętaj. Dlatego kluczowe znaczenie ma zatrudnianie i zatrzymywanie w zespole właściwych ludzi.

W szybkim rozwiązywaniu problemów, oprócz wiedzy technicznej, bardzo pomóc mogą umiejętności komunikacyjne pozwalające wyjaśniać luki w zabezpieczeniach i opisywać wpływ problemów na działalność biznesową. Najlepiej byłoby jeszcze, gdyby ten styl komunikacji obejmował opowiadanie ciekawych anegdotek, aby zaangażować zainteresowane strony.

Jednym z obszarów, które należy zbadać podczas rozmowy kwalifikacyjnej, są kwestie etyczne. Przywołaj scenariusz, który wymaga od pentestera podjęcia decyzji etycznej. Załóżmy, że zadaniem pentestera jest włamanie się do działu kadr lub wewnętrznego systemu nagradzania i oceny pracowników. Celem jest uzyskanie dostępu i wykazanie, czy możliwa jest eksfiltracja danych oraz czy istnieje system wykrywania włamań. Jak kandydat podejdzie do tego zadania? Czy

dokona eksfiltracji własnych rekordów albo rekordów innych pracowników, czy może zaproponuje eksfiltrację atrap rekordów albo będzie miał jeszcze inne pomysły? Sprawdź, czy kandydat postępuje zgodnie z wartościami, które chcesz widzieć w swoim programie, zespole i w Twojej organizacji.

Moim zdaniem, najlepszym sposobem na znajdowanie dobrych kandydatów są referencje, więc upewnij się, że pozostajesz w kontakcie z branżą. Bierz udział w konferencjach i rozpytuj, którzy kandydaci mogą być zainteresowani Twoją firmą.

Różnorodność i otwartość

Badanie dotyczące pracowników branży globalnego bezpieczeństwa informacji z 2017 r. (ang. *Global Information Security Workforce Study*) przedstawiło raport na temat aktualnego stanu kobiet w cyberbezpieczeństwie. Jednym z kluczowych wniosków było to, że kobiety stanowią 11% pracowników zajmujących się bezpieczeństwem informacji na świecie. Jeśli te liczby wydają się niskie, to dlatego, że takie są. A te 11% stanowi ten sam odsetek, co w 2013 r., a to oznacza, że w ostatnich kilku latach sytuacja nie uległa zmianie.

Szczegóły raportu można znaleźć tutaj: *https://blog.isc2.org/isc2_blog/2017/03/results-women-in-cybersecurity.html*.

Brak różnorodności jest widoczny podczas przechadzania się przez sale niektórych konferencji dotyczących bezpieczeństwa. Ponieważ konferencje te mają kluczowe znaczenie dla stanu infrastruktury sieciowej i rekrutacji, przyjazna atmosfera dla kobiet będzie bardzo przydatna.

Ponadto opracowanie *Global Information Security Workforce Study* podkreśla, że na stanowiskach niekierowniczych różnica w wynagrodzeniach zwiększyła się z 4% do 6%, a kobiety nieproporcjonalnie zajmują stanowiska niższego szczebla, a nie wyższego, menedżerskiego czy kierowniczego.

Co to oznacza dla testów penetracyjnych i czerwonych zespołów?

Aby zbudować silny i skuteczny program bezpieczeństwa ofensywnego oraz promować alternatywne analizy, posiadanie zróżnicowanego zestawu opinii, pomysłów i punktów widzenia jest naturalnym składnikiem sukcesu. W Twoim programie brakuje alternatywnych punktów widzenia i przeciwnych taktyk ze względu na brak wkładu ze strony żeńskich ekspertów ds. bezpieczeństwa.

Kierownictwo musi wynajdywać, wspierać i doceniać kobiety o wysokim potencjale poprzez zapewnienie możliwości szkolenia, mentoringu i zajmowania kierowniczych stanowisk. Ponadto pożądane jest, aby Twoja organizacja tworzyła grupy i organizowała spotkania poświęcone kobietom w dziedzinie bezpieczeństwa lub uczestniczyła w zewnętrznych tego typu grupach w internecie.

A jeśli jesteś na spotkaniu i widzisz, że kilka kobiet siedzi z boku, może dzieje się tak dlatego, że czują, iż nie mają głosu. Każdy może zaprosić i zachęcić je, by usiadły przy wspólnym stole. Chodzi o to, że wszystkie małe rzeczy mają znaczenie.

Morale i tożsamość zespołu

Zawsze chodzi o zespół. Dużą częścią sukcesu zespołu testów penetracyjnych jest morale i tożsamość. Aby zbudować tę tożsamość, pomocne może być posiadanie zgrabnej nazwy dla zespołu. I nie mam na myśli czegoś w rodzaju *Czerwony zespół <nazwa_firmy>* albo *Czerwony zespół <organizacja>*. Pentesterzy to kreatywne osoby, więc wymyślcie coś zabawnego, co będzie reprezentować to, kim jesteście i co zamierzacie zrobić! Oczywiście, z reguły przychodzi to samoistnie w sposób naturalny po przeprowadzeniu kilku wspólnych operacji.

W pewnym momencie mojej kariery utworzyłem zespół i postanowiłem nadać mu dość groźną nazwę. Wydawało się to dobrym pomysłem, a nazwa w naturalny sposób ewoluowała z uwagi na stosowanie pewnych zbudowanych wcześniej narzędzi. Utworzyłem więc ładne czerwone logo z żółtą czcionką. Siedziałem przez wiele godzin w nocy, zanim udało mi się przygotować pokaz slajdów, aby przekazać moim przełożonym ideę wewnętrznego zespołu bezpieczeństwa ofensywnego. Zasadniczo postępowałem zgodnie z wytycznymi, które omawiam w tej książce. Z mojego punktu widzenia wyglądało to na całkiem zgrabny pokaz slajdów.

Sama prezentacja nie przebiegła jednak gładko i długo nie wyszliśmy poza pierwszy slajd. Niestety, jednemu z członków kadry kierowniczej nie spodobały się nazwa zespołu ani jego logo. Doskonale pamiętam, jak ten dyrektor po spojrzeniu na slajd opuścił głowę i położył dłoń na czole. Uznał, że nazwa i logo zespołu ofensywnego były *zbyt mroczne* i nie chciał pozwolić na ich używanie. Pozostali dyrektorzy zapewnili jednak swoje poparcie, a wkrótce potem nastąpiła zmiana kierownictwa i wszystko potoczyło się tak, jak planowałem.

Od tego momentu wszystkie prace, operacje, narzędzia i projekty, nad którymi pracował zespół ofensywny, otrzymywały zabawne, a czasem urocze imiona, takie jak króliczek, wiewiórka itp. Szczególnie zabawne i pozytywne dla morale zespołu było otrzymywanie powiadomień i alertów informujących o wykryciu w środowisku *króliczków* i innych tego typu rzeczy.

Ostatecznie przeważył wzorzec wybierania nazw kodowych, a historia tej całej sytuacji, która do tego doprowadziła, stała się elementem wiążącym i tworzącym tożsamość zespołu. Nie brakowało też dobrych nazw dla przyszłych narzędzi i operacji.

Innym aspektem, który należy wziąć pod uwagę, jeśli chodzi o morale i tożsamość zespołu, jest ewentualny wpływ zespołu fioletowego (ściślej współpracy między zespołami czerwonym, niebieskim i inżynierskim), który będzie działał nieprawidłowo. Może to znacząco zagrozić tożsamości i morale czerwonego zespołu. Omówię to szerzej w rozdziale 3., „Mierzenie efektywności programu bezpieczeństwa ofensywnego", ale ważne jest, aby zachować zdrowe zróżnicowanie poglądów, a nie wykonywać po prostu zadania fioletowego zespołu.

Reputacja zespołu

Dla menedżera kluczowe znaczenie ma utrzymywanie w organizacji dobrej reputacji zespołu. Jeżeli zespół bezpieczeństwa ofensywnego został prawidłowo utworzony i jest odpowiednio prowadzony, rezultaty jego działania powinny być w całej organizacji doskonale dostrzegane. To od samego zespołu zależy, czy wykorzysta tę dostrzegalność i zdobyte dzięki niej możliwości w celu informowania właściwych zainteresowanych stron, aby napędzały wprowadzanie odpowiednich zmian i usprawnień.

Na dłuższą metę arogancka postawa nie pomaga. Może przysporzyć więcej szkód niż pożytku. To jeden z wczesnych etapów dojrzewania członka czerwonego zespołu. Niedojrzały czerwony zespół może np. przyjąć postawę defensywną, gdy zostanie przyłapany podczas działania. Przyglądanie się, jak zespół radzi sobie z „przyłapaniem" w trakcie przeprowadzania operacji, pomaga menedżerowi oceniać dojrzałość członków zespołu oraz samego programu. Poprzez obserwowanie interakcji między zespołem czerwonym a zespołem niebieskim w przypadku nieoczekiwanego wykrycia można się wiele nauczyć.

Bardziej doświadczony członek czerwonego zespołu przyjmie do wiadomości, że został wykryty, i pochwali osobę, która go przyłapała. Ponadto będzie starał się zrozumieć, jak do tego doszło, i spróbuje wyciągnąć nauczkę na przyszłość oraz wprowadzić odpowiednie usprawnienia. Dzięki wiedzy inżynierów produktu lub niebieskiego zespołu prawdopodobnie możliwe jest przeprowadzanie jeszcze skuteczniejszych ataków lub ich wariacji, które wskażą kolejne luki w zabezpieczeniach. Nikt nie jest wszechwiedzący, a informacje pozyskane dzięki innym osobom, patrzącym na sprawy z odmiennej perspektywy, mogą pomóc w zwiększeniu liczby wykrywanych problemów, którymi trzeba się zająć!

Okazywanie oznak arogancji i budowanie własnego ego to postawa, która nie jest rzadkością wśród nas — członków czerwonych zespołów. Gdy ma się do czynienia z silnym ego, potrzebne są dodatkowe elementy zarządzania oraz wprowadzenie coachingu, aby poprzez wywieranie jak największego wpływu zapewnić pełne wykorzystanie umiejętności i potencjału danej jednostki.

Najskuteczniejsi pentesterzy, jakich spotkałem, są skromni, ale asertywni, i potrafią przedstawić alternatywne punkty widzenia, aby zaskakiwać i edukować ludzi; przy tym nie są aroganccy i nie sprawiają wrażenia wszechwiedzących.

Świadczenie różnych usług na rzecz organizacji

Dobrze jest spojrzeć na program bezpieczeństwa ofensywnego pod tym kątem, że świadczy on organizacji różne usługi. Poznałeś pewnie czerwone zespoły, które koncentrują się na procesach biznesowych lub innych aspektach organizacji, tutaj skupimy się głównie na aspekcie cyberbezpieczeństwa.

Można powiedzieć, że świadczenie usług oznacza, iż naszymi klientami są inne grupy biznesowe, niebieskie zespoły i pracownicy organizacji. Tryby działania, odpowiedzialność i zadania zespołu przeprowadzającego testy penetracyjne mogą się znacznie różnić w zależności od zakresu obowiązków. Może on obejmować prace związane z projektowaniem i analizami, takie jak modelowanie zagrożeń, ale z pewnością powinien obejmować praktyczne ofensywne testy penetracyjne oraz wyszukiwanie i eksplorowanie luk w zabezpieczeniach w celach defensywnych. Większość tych usług dotyczy z reguły alternatywnych analiz.

W kolejnych punktach podrozdziału opisane zostały usługi, które zespół pentesterów może świadczyć swoim klientom. W bardzo dużych organizacjach usługi te mogą być zapewniane przez różne zespoły i grupy osób z wyznaczonymi obszarami zainteresowania, a czasami w jednej organizacji może istnieć nawet wiele zespołów świadczących podobne usługi (np. działające czerwone zespoły).

Wsparcie dla przeglądu zabezpieczeń i modelowania zagrożeń

Dobrą metodą na zaangażowanie zespołu bezpieczeństwa ofensywnego na wczesnym etapie jest korzystanie z jego usług w fazie projektowania systemu. Jest to najlepszy sposób na uzyskanie opinii przed wdrożeniem kodu lub ustaleniem procesów operacyjnych. Nawet jeśli systemy będą już wdrożone, nadal warto nadrobić zaległości i wykonać modelowanie zagrożeń dla systemów, środowisk i ludzi. Niektóre zespoły ofensywne mogą sprzeciwiać się włączeniu do prac na tym etapie, ponieważ różni się to nieco od ich misji.

Osobiście zawsze uważałem to za jeden z największych atutów posiadania wewnętrznego zespołu bezpieczeństwa ofensywnego. Gdy inżynierowie lub inne osoby w organizacji mają związane z bezpieczeństwem konkretne pytania dotyczące tego, jak zbudować określoną funkcjonalność lub opracować proces poprawiający bezpieczeństwo, zespół pentesterów może być świetną grupą do konfrontowania pomysłów i pomagania na wczesnym etapie ulepszania zabezpieczeń. Jeśli różne zespoły z całej organizacji zwracają się po poradę bezpośrednio do Twojego zespołu, to znaczy, że coś musiałeś zrobić tak, jak należy.

Ocena bezpieczeństwa

Zespół inżynierów może opracować nową funkcjonalność lub usługę i poprosić zespół ds. testów penetracyjnych o pomoc w ocenie stanu bezpieczeństwa i potencjalnych luk w zabezpieczeniach. To zadanie, które jest skoncentrowane bardziej na ocenianiu luk w zabezpieczeniach na poziomie aplikacji, a celem jest znalezienie jak największej liczby problemów za pomocą takich technik jak testy białej skrzynki i czarnej skrzynki. Niektórzy klasyfikują to jako przeprowadzanie klasycznych testów penetracyjnych.

Działania zespołu czerwonego

Jedną z najciekawszych rzeczy dla pentesterów może być prawdziwa praca czerwonego zespołu. Zazwyczaj są to tajne operacje, o których nie wiedzą zainteresowane strony, a działania są autoryzowane przez kierownictwo. W optymalnym przypadku zespół bezpieczeństwa ofensywnego sam określa cele, uzyskuje akceptację i przeprowadza testy.

W zależności od poziomu dojrzałości czerwonego zespołu i organizacji, warto naśladować bardzo konkretne ataki, aby rzucić wyzwanie niebieskiemu zespołowi (nazywa się to symulacją ataku hakerskiego). Taki atak może przybierać różne formy. Mogą to być symulacja konkretnego ataku hakerskiego, **zaawansowane trwałe zagrożenie** (ang. *Advanced Persistent Threat* — APT) w celu przeprowadzenia symulacji ataku na kryptowaluty lub fizyczne wtargnięcie do budynku w celu kradzieży własności intelektualnej. Działanie w czerwonym zespole jest zabawne i kreatywne — nie ma (a raczej nie powinno być) prawie żadnych zasad, jeśli w ogóle jakieś są.

Największym wyzwaniem dla dojrzałego czerwonego zespołu jest to, że prawdziwy przeciwnik łamie prawo. Czerwony zespół w swoich działaniach musi respektować przepisy prawne i reguły korporacyjne. Oczywiście, ma to wpływ na to, jak realistycznie można odgrywać pewne scenariusze — niektóre z nich powinny być odgrywane przynajmniej na papierze jako ćwiczenia symulacyjne.

Działania zespołu fioletowego

Zakres i cele działań zespołu fioletowego są bardzo podobne do działań określonych dla zespołu czerwonego. Podstawowa różnica polega na tym, że nacisk kładziony jest na przejrzystość i współpracę między zespołami czerwonym, niebieskim i inżynierskim. Celem na wszystkich etapach działania fioletowego zespołu jest prawie natychmiastowa poprawa stanu bezpieczeństwa systemu poprzez przeprowadzanie ataków oraz weryfikowanie mechanizmu wykrywania włamań i wysyłania alertów. Jeżeli ataki kończą się sukcesem i nie zostają wykryte, implementowane są poprawki mające na celu usunięcie luki w zabezpieczeniach, a ataki są natychmiast uruchamiane ponownie — aż do uzyskania wymiernej poprawy.

Działania fioletowego zespołu są jednym z najbardziej skutecznych sposobów na zapewnienie szybkiego rozwoju linii obronnej i zwiększenia dojrzałości organizacji, zwłaszcza jeśli istnieje wewnętrzny zespół bezpieczeństwa ofensywnego, który może współpracować z zespołem niebieskim. Korzyści płynące ze ścisłej współpracy i wykorzystania przewagi działania na własnym terenie omówię szerzej w następnym rozdziale.

Pamiętaj, aby stale kwestionować własne sposoby działania oraz przekonania. Ideą ofensywnego bezpieczeństwa i alternatywnej analizy jest podważenie status quo.

Poprzez łączenie działań zespołu fioletowego i niejawnych działań zespołu czerwonego można upewnić się, że ktoś weryfikuje ataki bez (prawie) żadnych ograniczeń. Jeśli większość organizacji zapewnia działanie tylko fioletowego zespołu, powstaje potrzeba zatrudnienia jakiegoś zewnętrznego zespołu czerwonego do przeprowadzenia testów penetracyjnych. Można by rzec, że staje się to dla fioletowego zespołu pewnym sprawdzianem, który weryfikuje, czy udało im się poprawić system bezpieczeństwa organizacji.

Ćwiczenia symulacyjne

Czasami odegranie pewnych scenariuszy ataku w sposób operacyjny nie jest możliwe lub wykonalne. Może to wynikać z braku dostępnych zasobów, kwestii prawnych lub ograniczeń technicznych. Dobrą i dość tanią alternatywą jest przeprowadzanie **ćwiczeń na papierze** przy udziale kluczowych zainteresowanych stron. Ćwiczenia symulacyjne mogą być świetną okazją, aby zaangażować kadrę kierowniczą wyższego szczebla oraz radę nadzorczą w badanie scenariuszy ataków i zachęcić ich do czynnego udziału oraz wskazywania luk w zabezpieczeniach.

Badania i rozwój

Do tej kategorii można zaliczyć dwa podstawowe obszary, z których pierwszy to badania dotyczące bezpieczeństwa oraz luk w zabezpieczeniach. Jest to główny priorytet zespołu bezpieczeństwa ofensywnego. Obejmuje badania nad nowymi lukami w zabezpieczeniach i nowymi klasami luk w tychże zabezpieczeniach. Drugi obszar to tworzenie narzędzi i exploitów w celu wskazywania konsekwencji eksploatacji luk w zabezpieczeniach oraz testowanie możliwości mechanizmu wykrywania włamań. Narzędzia te będą używane podczas działań zespołu czerwonego do testowania środków zaradczych wprowadzonych w celu wykrywania ataków i obrony przed nimi. Celem zespołu czerwonego jest wymuszanie opracowywania poprawek dla luk w zabezpieczeniach i upewnianie się, że jeśli prawdziwi hakerzy opracują podobne exploity, zostaną one wykryte.

Predykcyjna analiza ataków i wsparcie dla reagowania na incydenty

Jeśli dojdzie do incydentu naruszenia bezpieczeństwa, zespół bezpieczeństwa ofensywnego może pomóc w określeniu tego, czego szuka aktywny haker. Zespół prawdopodobnie będzie mógł przewidzieć następny krok przeciwnika ze względu na unikatowy sposób myślenia atakującego. A tak przy okazji, uznanie za ukucie terminu **predykcyjna analiza ataków** (ang. *predictive attack analysis*) należy się Farzanowi Karimiemu. Jest to część przewagi działania na własnym terenie, jaką może zapewnić wewnętrzny zespół bezpieczeństwa ofensywnego, a w sytuacjach kryzysowych zespół ten może dostarczyć kluczowych informacji, które pozwolą być o krok przed hakerem.

Dodatkowe obowiązki programu ofensywnego

Do tej pory wskazałem kilka podstawowych zadań, które powinny być wykonywane w ramach programu czerwonego zespołu. Istnieją jednak jeszcze dodatkowe obowiązki, którym warto się przyjrzeć, ponieważ mogą ewentualnie zostać włączone do programu. Omówię teraz szerzej niektóre z nich.

Edukacja i szkolenie w zakresie bezpieczeństwa

Zespół bezpieczeństwa ofensywnego może pomóc w zmianie kultury organizacji i poprawić ogólne IQ bezpieczeństwa. W ramach wykonywania swoich zadań pentesterzy pozyskują określone informacje o ludziach, procesach i technologiach organizacji. Zespół ofensywny ma również silną pozycję do zapoczątkowania zmian kulturowych i poszerzenia unikatowej wiedzy organizacji na temat bezpieczeństwa.

Zwiększenie IQ bezpieczeństwa organizacji

Równolegle z edukacją i zapewnianiem szkoleń, zadaniem programu ofensywnego powinno być podnoszenie IQ bezpieczeństwa całej organizacji, w tym zespołów niebieskich, zespołów zajmujących się usługami i produktami, działu kadr i księgowości.

Gromadzenie informacji o zagrożeniach

Jednym z zadań, jakie może należeć do programu ofensywnego, jest zbieranie informacji o zagrożeniach w celu zrozumienia aktualnych trendów w ofensywnym bezpieczeństwie, poznania aktywnych aktorów zagrożeń oraz nowych technik, narzędzi lub procesów, które ci aktorzy obecnie tworzą lub wykorzystują.

Bycie na bieżąco z najnowszymi trendami i zagrożeniami oraz pozyskiwanie wiedzy, jakie dane związane z organizacją dostają się do tzw. ciemnej sieci (ang. *Dark Web*), będzie zadaniem zespołu czerwonego zwłaszcza w mniejszych organizacjach, które nie mają specjalnego programu zbierania informacji wywiadowczych o zagrożeniach.

Informowanie grup zarządzania ryzykiem i kierownictwa

Kolejnym obszarem, w który powinien zaangażować się czerwony zespół, jest kształtowanie procesu zarządzania ryzykiem w organizacji i wnoszenie do niego aktywnego wkładu. Zagrożenia dla bezpieczeństwa informacji mogą nie zostać prawidłowo uwzględnione, gdy zainteresowane strony będą omawiać ryzyko, na jakie narażona jest firma.

Program ofensywny może zapewnić informacje dotyczące wrogiej aktywności, która może mieć negatywny wpływ na kluczowe obszary prowadzonej działalności. Ponadto program ten może wskazywać wadliwe procesy, gdzie zbyt wiele osób ma nieograniczony dostęp do informacji, lub funkcjonalności, które mogą przypadkowo negatywnie wpłynąć na działalność firmy i spowodować trwałe szkody z powodu ludzkiego błędu bez wrogiego zamiaru.

Branża bezpieczeństwa koncentruje się na pomiarach jakościowych i wskaźnikach bezpieczeństwa. Potrzebne są jednak bardziej znaczące sposoby wyrażania ryzyka. W rozdziale 3., „Mierzenie efektywności programu bezpieczeństwa ofensywnego", omówię inne koncepcje związane z określaniem ryzyka.

Integracja z procesami inżynieryjnymi

Wskazane jest, aby program zespołu czerwonego zakładał integrację i regularną komunikację z zespołem inżynierów i innymi odpowiednimi zainteresowanymi stronami, aby przeprowadzać ewaluację stanu bezpieczeństwa. Jeśli taka współpraca nie istnieje, czas nad nią popracować. Brak wglądu w określone informacje jest często powodem, dla którego luki w zabezpieczeniach, jakie można było wcześniej wykryć i usunąć, nie docierają do środowiska produkcyjnego. Mniejsze organizacje mogą potrzebować takiego zaangażowania raz w roku, natomiast duże organizacje komercyjne mogą korzystać z wielu ewaluacji rocznie.

Taka integracja zapewnia regularne przeprowadzanie ocen stanu bezpieczeństwa, a zespół ds. bezpieczeństwa może dzięki niej planować bardziej złożone operacje czerwonego zespołu, które wykorzystują i integrują najnowsze systemy oraz usługi zbudowane w celu dostarczenia największej wartości.

Kolejną koncepcją w tym zakresie jest przeprowadzanie okresowych ćwiczeń ofensywnych dla każdej grupy biznesowej.

Mam wrażenie, jakbym Cię znał — zrozumienie etycznych aspektów działań czerwonego zespołu

Faktycznie jest to tak przerażające, jak się wydaje, i niewiele się o tym mówi, mimo że dla inżynierów bezpieczeństwa ofensywnego jest to rzeczywistość. Inżynier bezpieczeństwa w końcu poznaje różne sekrety i nienaprawione luki w zabezpieczeniach. Obejmuje to hasła wybierane przez pracowników organizacji. Z tą wiedzą wiążą się poważne względy etyczne oraz profesjonalizm, którymi muszą wykazać się inżynierowie bezpieczeństwa.

Może to doprowadzić do naprawdę dziwnych i stresujących sytuacji — wyobraź sobie, że dowiadujesz się, iż ktoś używa hasła *N!eChceJuzDluzejZyc!*. Albo wyobraź sobie inżyniera bezpieczeństwa ofensywnego, który podczas operacji natrafia na nielegalne treści. Ponadto istnieje pewne prawdopodobieństwo, że w czasie wykonywania codziennych obowiązków inżynier bezpieczeństwa ofensywnego natknie się na prawdziwego hakera.

Jak już wspomniałem, nie jest to coś, o czym się szeroko dyskutuje, a nabywana wiedza powoduje pewien stres związany z potencjalnymi informacjami o ludziach, procesach i technologiach, które stawiają inżynierów bezpieczeństwa ofensywnego przed dylematami etycznymi. Zadaniem menedżera jest również zapewnienie inżynierom bezpieczeństwa ofensywnego możliwości szukania wskazówek i porad (zarówno u prawników, jak i psychologów). Ponadto, jeśli ktoś używa służbowego komputera do celów prywatnych, takich jak bankowość lub poczta e-mail, inżynier ofensywny także może w sposób niezamierzony uzyskać dostęp do danych osobowych takiego pracownika. Zasady przeprowadzania testów penetracyjnych i standardowe procedury operacyjne mają pomóc w rozwiązywaniu takich problemów i zostaną opisane dalej w tej książce.

Stwierdzenie: „Mam wrażenie, jakbym Cię znał" jest autorstwa jednego z najlepszych członków czerwonych zespołów, z którymi miałem okazję pracować przez lata — Ty wiesz, że chodzi o Ciebie.

Szkolenie i edukacja zespołów bezpieczeństwa ofensywnego

Ten aspekt jest często w organizacjach niedoinwestowany. Aby zbudować silny program bezpieczeństwa ofensywnego i przyciągnąć talenty, ważna jest dostępna jasna ścieżka edukacji dla członków zespołu, aby mogli rozwijać zarówno indywidualne aspiracje zawodowe, jak i sam program. Obejmuje to możliwość uczestniczenia w konferencjach dotyczących bezpieczeństwa, aby uczyć się i nawiązywać kontakty, ale także prezentować własne badania oraz inspirować się pracą innych i wymyślać kolejne doskonałe pomysły lub działania.

Często zdarza się nam utknąć w ciągłej pracy operacyjnej i zapominać o szkoleniach. Istnieje świetna analogia, którą kiedyś usłyszałem od mentora. O ile wiem, historia ta opiera się na tym, co powiedział Abraham Lincoln.

Pewien drwal cały dzień ciął drewno. Z biegiem czasu jego siekiera się stępiła. Drwal stopniowo stawał się coraz wolniejszy w cięciu drewna. Był po prostu zbyt zajęty cięciem drewna, żeby naostrzyć siekierę! Pewnego dnia przyjaciel powiedział mu: „Hej człowieku, ostatnio byłem znacznie bardziej produktywny w cięciu drewna niż Ty. Myślę, że powinieneś naostrzyć swoją siekierę i znowu będziesz dużo szybszy!". Odpowiedź drwala była prosta i jednoznaczna: „Nie mam na to czasu, jestem zajęty cięciem drewna!".

Jaki jest morał tej historii? Nie trać z oczu szerszej perspektywy, zwłaszcza jako lider programu ofensywnego. Zachęcaj członków swojego zespołu, aby stali się czynnymi działaczami społeczności bezpieczeństwa, uczyli się od innych, a także przekazywali swoją wiedzę. Dzięki temu społeczność bezpieczeństwa w Twojej organizacji i poza nią będzie mogła na tym skorzystać, a my będziemy mieli pewność, że nasze dane są dobrze chronione i bezpiecznie obsługiwane we wszystkich organizacjach. Jesteśmy w tym razem!

Kilka z moich najlepszych pomysłów na napisanie narzędzi było wynikiem uczestnictwem w takich konferencjach jak Blackhat, Defcon czy Chaos Communication Congress. To środowisko jest bardzo inspirujące. Pomaga ćwiczyć umysł, otwierać się na kreatywne pomysły i wracać do biura z dużą motywacją.

Zasady, reguły i standardy

Twoja organizacja prawdopodobnie ma już wdrożone zasady dotyczące przeprowadzania testów bezpieczeństwa, chociaż prawdopodobnie w inny sposób, niż mógłbyś oczekiwać. Na początkowym etapie jakakolwiek forma testów penetracyjnych jest najprawdopodobniej wyraźnie zabroniona! Aby umożliwić działania inżynierii bezpieczeństwa ofensywnego, konieczne jest rozszerzenie tych zasad i standardów, aby zapewnić zespołowi ofensywnemu framework do wykonywania jego obowiązków.

Te zasady i standardy mają również chronić zespół bezpieczeństwa ofensywnego i zagwarantować mu możliwość pracowania w ramach ustalonego i autoryzowanego zestawu reguł. Jako menedżer programu powinieneś również upewnić się, że każdy, kto prowadzi objęte nim działania, zapoznał się z tymi zasadami i zgodził się ich przestrzegać. Również w tym przypadku w Twojej organizacji może już istnieć ustalona procedura. Jeśli nie, postaraj się śledzić tę kwestię.

Zasady, którymi należy się kierować, i reguły, których należy przestrzegać

Przeprowadzanie testów penetracyjnych i zapewnianie bezpieczeństwa ofensywnego to jedne z najbardziej ekscytujących zadań, jakie można wykonywać. Jest to praca wymagająca umiejętności, kreatywności, dociekliwości i poświęcenia.

Aby jak najlepiej wykorzystać program bezpieczeństwa ofensywnego, ważne jest zdefiniowanie zestawu zasad, które podkreślają wartości i cele zespołu bezpieczeństwa ofensywnego. Zasady te mają poprowadzić Cię, gdy wkroczysz na nieznane terytorium, a z takimi sytuacjami mają regularnie do czynienia inżynierowie bezpieczeństwa ofensywnego.

Działanie z określonym celem i zachowanie pokory

Po latach bycia pentesterem i menedżerem ds. inżynierii bezpieczeństwa ofensywnego, prowadzącym duże operacje z dziesiątkami zainteresowanych stron, chciałbym zaoferować Ci kilka rad, które mogą pomóc w wywieraniu znaczącego, pozytywnego wpływu na innnych. Po prostu dobrze się baw, zachowaj pokorę i staraj się dopingować ludzi do działania.

Unikaj postawy defensywnej lub aroganckiej — działasz w końcu po stronie ofensywnej, po stronie mocy, po stronie, która może napędzać zmiany i kierować nimi. Postaraj się zapoczątkować tę zmianę w Twojej organizacji i zainspirować ją do zrozumienia oraz przyjęcia alternatywnych poglądów, a także zaakceptowania istnienia słabych punktów. Zachęcaj współpracowników, aby pomagali Ci znajdować warianty różnych problemów. Rozważ dostosowanie własnych poglądów do innych punktów widzenia. Zawsze zakładaj, że jest coś, czego nie wiesz.

Testy penetracyjne są reprezentatywne, ale nie wyczerpujące

Testowanie nigdy się nie kończy. Testy bezpieczeństwa i testy penetracyjne nie stanowią wyjątku. Zawsze znajdzie się jakiś kolejny błąd, który będzie można wykryć, stosując większą ilość zasobów. Podstawowym obowiązkiem jest inwestowanie i działanie z należytą starannością, aby możliwe było wykrywanie obszarów stanowiących najbardziej znaczące ryzyko.

Pentesting nie zastępuje funkcjonalnego testowania bezpieczeństwa

Najmniej pożądanym wynikiem przeprowadzania testów penetracyjnych jest znajdowanie luk w zabezpieczeniach, które ewidentnie stanowią funkcjonalne problemy związane z bezpieczeństwem, takie jak brak autoryzacji lub nieprawidłowe zachowanie autoryzacji.

Zespół bezpieczeństwa ofensywnego powinien wyznaczyć granicę, aby najpierw określać oczekiwania dotyczące jakości oprogramowania. Dlatego pomiar wyników testów penetracyjnych dla poszczególnych zespołów zajmujących się komponentami lub usługami może dostarczyć wielu informacji, ponieważ dane rozłożone w czasie mogą wskazywać, że niektóre zespoły w organizacji wykazują określone wzorce. Przed zaangażowaniem zespołu bezpieczeństwa ofensywnego zespoły te mogą skorzystać z dodatkowego szkolenia, dodatkowego przeglądu projektu lub reguł zapewnienia jakości.

Umożliwienie pentesterom eksploracji

Pentesterzy potrzebują niezależności, żeby nie musieli robić tego, czego chcą inni. Wielu wyjątkowych inżynierów testowych i członków czerwonych zespołów działa, opierając się na intuicji i przeczuciu. Nie należy tego uniemożliwiać lub blokować. Nadrzędne reguły i zasady mają na celu umożliwienie i ochronę tego zachowania oraz zapewnienie odpowiedzialności wszystkich zainteresowanych stron.

Informowanie grup zarządzających ryzykiem

Ostatnia zasada, którą należy przekazać zespołowi, jest taka, że ich celem jest pomoc w informowaniu właścicieli firmy o ryzyku biznesowym. Jakie scenariusze mogą najbardziej zaszkodzić firmie? Zadaniem zespołu bezpieczeństwa ofensywnego jest ich wskazywanie, usunięcie niepewności dotyczącej istnienia problemów oraz zwiększanie stopnia zrozumienia zagrożeń przy jednoczesnym zmniejszaniu prawdopodobieństwa ich wystąpienia.

Zasady przeprowadzania testów penetracyjnych

Zestaw jasnych zasad przeprowadzania testów penetracyjnych (ang. *Rules of Engagement* — ROE) powinien zostać ustanowiony oraz zatwierdzony przez kierownictwo i dział prawny, aby zapewnić, że do efektywnej symulacji i emulacji działań przeciwników oraz ataków mogą być stosowane określone narzędzia, techniki i procedury. Wybitny zespół testerów penetracyjnych staje się odpowiedzialny za zachowywanie najwyższych możliwych standardów i działa z dołożeniem wszelkich należytych starań. Dotyczy to również etyki biznesowej.

Dlatego ważne jest ustalenie zasad, których zespół będzie przestrzegał. Oto kilka przykładów.

- Czyń dobro! Zawsze działaj z należytą starannością.
- Bez wyraźnego upoważnienia nie przeprowadzaj testów typu „odmowa usługi” (ang. *Denial of Service* — DoS) ani nie odmawiaj celowo dostępu do systemów.
- Przed przeprowadzaniem hakowania zasobów ustal z zainteresowanymi stronami listę celów zabronionych (ang. *no-strike list*). **Lista celów zabronionych to zestaw zasobów lub systemów, które są poza zasięgiem dla zespołu przeprowadzającego testy penetracyjne**.
- Działaj raczej chirurgicznie zamiast przeprowadzać naloty dywanowe.
- Podczas przeprowadzania operacji i po ich zakończeniu poświadczenia i inne wrażliwe artefakty bezpieczeństwa obsługuj w sposób bezpieczny i zabezpieczony.
- Zamiast uzyskiwać dostęp do danych klientów, eksfiltruj dedykowane rekordy danych. Dedykowane rekordy danych to w zasadzie atrapy danych, które są tworzone jako cel dla zespołu przeprowadzającego testy penetracyjne.
- Szanuj prywatność pracowników.
- Wycofaj się i wstrzymaj działania, gdy zostaniesz o to poproszony przez właścicieli firmy lub kierownictwo niebieskiego zespołu.

Inną kwestią, na którą należy zwrócić uwagę, jeśli chodzi o zasady przeprowadzania testów penetracyjnych, jest reguła **pokazywania kart** przez pentesterów, gdy poprosi o to kierownictwo niebieskiego zespołu. Reguła ta zależy w dużej mierze od dojrzałości programu zespołu

czerwonego i jego członków, ale generalnie jest to prawidłowe podejście długoterminowe. Zasady te mają znaczenie w przypadku, gdy w organizacji aktywny jest prawdziwy haker, a zespół niebieski musi odróżnić go od zespołu czerwonego.

Dobrym źródłem pomysłów na tworzenie reguł jest badanie programów nagradzania za wyszukiwanie błędów prowadzonych przez różne firmy oraz podręcznik *San Remo Handbook on Rules of Engagement* (*www.iihl.org/sanremo-handbook-rules-engagement*). Podręcznik San Remo jest zgodny z restrykcyjnym podejściem do autoryzacji — jeśli coś nie jest wyraźnie dozwolone, jest zabronione.

Jako doświadczony członek czerwonego zespołu powinieneś również zapytać o zasady przeprowadzania działań zespołu niebieskiego. Ma on dostęp do wielu informacji (kto przegląda określone strony internetowe, jakie procesy są uruchamiane na poszczególnych maszynach itd.) i często nie działa na podstawie jasnych zasad przeprowadzania działań.

Na koniec warto jeszcze dodać, że zasady i procedury należy regularnie weryfikować i dostosowywać, jeśli trzeba.

Dostosowywanie zasad przeprowadzania testów penetracyjnych do operacji

Zasady przeprowadzania testów penetracyjnych mogą różnić się w przypadku każdej operacji. Czasami dopuszczalne mogą być pewne aspekty ataków — np. podczas symulacji ataku DoS na określony cel — których normalnie nie byłoby na liście zatwierdzonych technik.

Czasami zamiast chirurgicznego działania może być wymagana operacja masowego hakowania zasobów. Luki w zabezpieczeniach, takie jak np. WannaCry lub Slammer, umożliwiły automatyczne wykrywanie dodatkowych celów i rozpowszechnianie się w ten sposób w całej sieci organizacji. Czerwony zespół może mieć zamiar przeprowadzenia bezpiecznej emulacji takiego złośliwego oprogramowania, aby zademonstrować zasięg rażenia i wpływ luk w zabezpieczeniach. Dla wszelkich takich operacji kluczowe znaczenie ma — oczywiście — wprowadzanie zabezpieczeń i tymczasowych rozwiązań.

Gdy testowanie może potencjalnie obejmować zewnętrzną usługę, zawsze należy wziąć pod uwagę specjalne względy. Konieczne mogą być dodatkowa autoryzacja i (lub) powiadomienia.

Geograficzne i jurysdykcyjne obszary działania

Zasady przeprowadzania testów penetracyjnych powinny uwzględniać również obszary działania, aby zapewnić, że podczas przeprowadzania operacji zespół nie naruszy żadnych lokalnych zasad i przepisów prawnych. Wszelkie takie zasady należy skonsultować z doradcą prawnym.

Ograniczenia prawne lub reguły lokalnych firm dotyczące tego, jakie taktyki i techniki mogą być stosowane w organizacji w Niemczech, mogą się różnić np. w porównaniu z tym, co jest dozwolone podczas przeprowadzania testów penetracyjnych w Stanach Zjednoczonych lub w Chinach. Pracownicy mają swoje prawa, w tym prawo do prywatności. Zawsze należy upewnić się, że działania zostały autoryzowane i zasięgnięto porady prawnej.

Jednym z argumentów przy omawianiu tych kwestii jest zawsze to, że prawdziwy haker nie ma tych ograniczeń. I ten argument jest słuszny, ale gdy prawdziwy haker zostanie złapany, pójdzie do więzienia, a autoryzowany pentester nie.

Dystrybucja materiałów informacyjnych

Dobrą praktyką wymienioną w podręczniku San Remo jest opracowywanie dla członków zespołu ulotek informacyjnych, które będą zawierać również zasady przeprowadzania testów penetracyjnych — będą się nimi kierować podczas przeprowadzania operacji. Może to, oprócz wartości praktycznej, również pomóc w poprawieniu morale i tożsamości zespołu. Można np. rozważyć umieszczenie na ulotkach również logo i nazwy zespołu lub przygotowanie spersonalizowanej monety albo jeszcze lepiej może jakiejś zabawnej płytki drukowanej.

Prawdziwe, symulowane i emulowane ataki

Członkowie Twojego czerwonego zespołu z pewnością zwrócą uwagę, że haker w prawdziwym świecie nie ma ograniczeń dotyczących wrogich taktyk, technik i procedur, z których może korzystać. Prawdziwy przeciwnik nie musi przestrzegać opisanych wcześniej zasad przeprowadzania testów penetracyjnych ani innych ograniczeń prawnych czy reguł zgodności. Może np. ukraść hasła Twoich pracowników w Europie i podszywać się pod ich tożsamości w sieci w taki sam sposób, jak w przypadku pracowników w Stanach Zjednoczonych czy Chinach. Ze względu na różnice w przepisach dotyczących prywatności, zasadach firmy i uregulowaniach prawnych mogą istnieć różnice dotyczące możliwości i sposobu emulowania tych ataków przez zespół bezpieczeństwa ofensywnego. Zanim zaczniesz emulować ataki przeciwników, skonsultuj się z doradcą prawnym.

Jeśli z jakiegoś powodu Twoja organizacja zabrania emulowania taktyk prawdziwych ataków, musisz kontynuować dyskusję w tej kwestii, ponieważ prawdziwi przeciwnicy prawdopodobnie robią to właśnie w tej chwili, a Twoja organizacja ma dość spory martwy punkt w tym obszarze. Wartość edukacyjna dla wszystkich stron zaangażowanych w operację czerwonego zespołu będzie podnosić IQ bezpieczeństwa organizacji i umożliwi poszczególnym pracownikom lepszą ochronę przed tymi atakami.

W przypadku niektórych testów można tworzyć środowiska symulacyjne lub wdrażać dane testowe (atrapy danych) w celu przeprowadzenia ataków i eksfiltracji. Czasami również samo przeprowadzenie operacji na papierze może dostarczyć cennych i tanich w pozyskaniu informacji. Przeprowadzenie kampanii phishingowej nie zawsze musi oznaczać faktyczną kradzież haseł

użytkowników. Cenną lekcją może być samo nakłonienie pracowników do wprowadzenia swoich danych uwierzytelniających na stronie phishingowej i wyświetlenie ostrzeżenia po naciśnięciu przycisku zatwierdzenia.

Żadna z tych symulacji nie zapewnia jednak takiej samej wartości i obserwacji, jak wykonanie realistycznego ataku na system produkcyjny w celu wykazania rzeczywistych braków w systemie bezpieczeństwa i wykrywania włamań.

Porównanie systemów produkcyjnych i nieprodukcyjnych

Prowadzi to do pytania, czy celami ataków powinny być środowiska produkcyjne, czy testowe. Mniej dojrzałe organizacje są z reguły niechętne przeprowadzaniu jakichkolwiek testów penetracyjnych w środowiskach produkcyjnych. Jest to zwykle dobry wskaźnik, że dana usługa wymaga jeszcze sporo pracy, aby stała się prawdziwie odporna i dojrzała.

Proste skanowanie portów lub fuzzing nie powinny mieć żadnego wpływu na dostępność usługi, a dojrzały system może wytrzymać takie testy bez żadnych problemów. Jeżeli fuzzing ma zauważalny wpływ na dostępność, jest to ważne odkrycie pokazujące, że zespół inżynierów nie uwzględnił z wyprzedzeniem tego rodzaju pracy.

Dobrym pomysłem jest zwykle zbadanie raportów z oceny bezpieczeństwa w środowiskach produkcyjnych, zwłaszcza ze względu na ewentualną błędną konfigurację oraz różnice między systemami produkcyjnymi i nieprodukcyjnymi.

Często zdarza się także, że systemy produkcyjne i testowe pokrywają się. Może to wynikać z wykorzystywania danych produkcyjnych w środowisku testowym lub współdzielenia haseł i certyfikatów między tymi dwoma środowiskami. Z tego punktu widzenia na ogół właściwym podejściem jest uwzględnienie podczas operacji środowisk produkcyjnych i nieprodukcyjnych.

Unikaj zostania pionkiem w politycznej rozgrywce

Może się zdarzyć, że czerwony zespół będzie używany jako pionek w rozgrywkach służących osiągnięciu celów kilku osób, zamiast wspierać całą organizację i pomagać w poprawie kultury i świadomości bezpieczeństwa. Miej tę świadomość i staraj się tego unikać.

Standardowa procedura operacyjna

W celu opisania ogólnego przepływu pracy podczas przeprowadzania testu penetracyjnego lub operacji bezpieczeństwa ofensywnego tworzona jest **standardowa procedura operacyjna** (ang. *Standard Operating Procedure* — SOP). Obejmuje ona zainteresowane strony, osoby autoryzujące, informowane strony, inne uczestniczące podmioty oraz cele operacji. Procedura

SOP jest ważna dla zapewnienia rozwoju dojrzałego i powtarzalnego procesu. Podobnie jak w przypadku zasad przeprowadzania testów penetracyjnych, wskazane jest zasięgnięcie porady prawnej, aby upewnić się, że wskazane taktyki i techniki nie naruszają reguł firmy lub przepisów prawnych.

Należy uwzględnić określone kwestie dotyczące całego zlecenia, a procedury mogą się różnić w zależności od tego, co oferuje usługa opisywana przez konkretną procedurę. Na rysunku 1.1 przedstawiłem niektóre podstawowe kwestie dotyczące usługi fioletowego zespołu. Wiele z tych etapów i procedur ma również zastosowanie do zespołów czerwonych i usług testów penetracyjnych.

Rysunek 1.1. Standardowa procedura operacyjna

Przydatne jest tworzenie szablonów SOP w celu uzyskania powtarzalnego procesu i możliwości ponownego wykorzystania formatu.

Wykorzystywanie planów ataków do śledzenia operacji

Plan ataku to ogólny podstawowy plan testów służący do śledzenia operacji. Powinien zawierać wszystkie informacje niezbędne do śledzenia logistyki, zainteresowanych stron, zadań i ustaleń, oraz udostępniania notatek. Może bezpośrednio zawierać różne dane lub, jeśli trzeba, wskazywać inne dokumenty.

Cel misji — co zamierzamy osiągnąć lub zademonstrować?

Cel misji będzie jasno określał zamiar operacji. Jasny cel misji będzie niezwykle pomocny, ponieważ pomoże pentesterom skupić się na właściwych celach ataku i zastosować odpowiednie techniki.

Podejście i tryb działania pentesterów będą zupełnie inne w zależności od konkretnego celu misji, np. gdy celem misji będzie wykonanie przez czerwony zespół włamania, w celu oceny gotowości systemu wykrywania włamań przez wykradzenie określonej produkcyjnej bazy danych, albo gdy zadanie będzie polegało na ocenieniu stanu bezpieczeństwa i możliwości wykrywania włamań dedykowanej strony internetowej.

Cele podstawowe powinny również obejmować cele pośrednie, takie jak uniknięcie wykrycia lub wykorzystanie wyłącznie taktyki określonego dobrze znanego przeciwnika. Pomaga to w ocenie operacji poprzez ewaluację nie tylko ogólnego celu operacji, ale również celów pośrednich oraz ich zdolności wykrywania włamań lub reagowania na nie.

Ogólny cel misji może zostać ustalony podczas spotkania z zainteresowanymi stronami biznesowymi lub samodzielnie zdefiniowany przez zespół bezpieczeństwa ofensywnego.

Zainteresowane strony i ich obowiązki

Poniżej wymieniony został zestaw ról, które należy określić i zdefiniować, aby zapewnić wykonywanie dobrze udokumentowanych i efektywnych operacji.

- **Zespół usługi lub produktu** — jakie cele zostały uwzględnione?
- **Zainteresowane strony biznesowe** — kto jest właścicielem celu?
- **Zespół niebieski** — w zależności od rodzaju operacji można włączyć do niej zespół niebieski.
- **Zespół czerwony** — to my!
- **Autoryzacja** — kto autoryzował operację? Zwykle obejmuje to zainteresowane strony biznesowe.
- **Informowane strony** — inne podmioty, które powinny być informowane o podejmowanych działaniach i otrzymywać sprawozdania oraz ustalenia.

Jeśli Twoja firma nie utrzymuje własnej infrastruktury, ale korzysta z systemów chmurowych, upewnij się, że masz odpowiednią autoryzację od dostawcy usług w chmurze, aby przeprowadzić na nich testy bezpieczeństwa ofensywnego. Niektóre firmy, takie jak Amazon, mogą wymagać dopełnienia pewnych formalności.

Aby zdefiniować zainteresowane strony i ich role, można wykorzystać również prostą macierz odpowiedzialności zwaną RACI (ang. *Responsible*, *Accountable*, *Consulted*, *Informed*, co w wolnym tłumaczeniu przekłada się na następujące elementy: „osoba ponosząca odpowiedzialność operacyjną", „osoba ponosząca odpowiedzialność służbową", „konsultanci" oraz „informowane strony"). Więcej informacji na temat tej metody znajdziesz w dokumencie *Roles & Responsibility Charting* autorstwa Michaela L. Smitha i Jamesa Erwina (*https://pmicie.org/files/22/PM-Toolkit/85/racirweb31.pdf*).

Oto prosta macierz RACI służąca do zdefiniowania ról i obowiązków dla działania zespołu czerwonego.

	Opis	Osoby
Odpowiedzialność operacyjna	Osoby odpowiedzialne za wykonywanie zadań operacyjnych procedury	Mallory Miller Eve Dropper
Odpowiedzialność służbowa	Osoba odpowiedzialna za wykonaną pracę	Dyrektor działu testów penetracyjnych i czerwonego zespołu
Konsultanci	Osoby i elementy zaangażowane do współpracy, takie jak kierownik grupy inżynierów, testowany produkt lub (w przypadku operacji zespołu czerwonego) kierownictwo zespołu odpowiedzialnego za testowany produkt	Tom Builder Susane Coder Sarach Sequel
Informowane strony	Grupa, która powinna być informowana o głównych decyzjach (np. za pomocą powiadomień lub dostarczania sprawozdań)	Grupa produktowa

Kryptonimy

Każdej operacji (szczególnie przeprowadzanej przez zespół czerwony) należy przypisać kryptonim odnoszący się do wykonywanych działań i planowanych celów, który będzie umożliwiał zainteresowanym stronom komunikowanie się w danej sprawie bez konieczności ciągłego ujawniania celów ataków i celów misji.

Dobre kryptonimy pomagają również w tworzeniu silnego poczucia wspólnoty i tożsamości zespołu. Ponadto wprowadzają do pracy element zabawy, a czym byłoby nasze życie, gdybyśmy nie mogli się trochę zabawić?

Harmonogram i czas trwania

Czas trwania operacji bezpieczeństwa ofensywnego może być bardzo różny. Taka operacja może trwać kilka dni, wiele tygodni, a nawet miesięcy. W tym przypadku nie ma żadnej reguły ani najlepszej praktyki. Zależy to wyłącznie od celu misji oraz tego, jakie mają być cele ataków, strategiczne wyniki lub zmiany organizacyjne.

Warto uwzględnić w planie dodatkowy czas na wypadek, gdyby zmodyfikowane zostały cele misji lub dodane nowe cele ataków. Należy analizować te kwestie w miarę postępu operacji, otrzymywania nowych danych wywiadowczych i odkrywania kolejnych rzeczy. Może to nawet oznaczać przerwanie misji, aby najpierw zmienić jej priorytety.

W przypadku ogólnych ocen bezpieczeństwa dobrze jest zarezerwować przynajmniej kilka tygodni. Zależy to od wielkości i zakresu celu. Operacje zespołów czerwonych mogą trwać dłużej, nawet miesiące, ale prowadziłem z czerwonymi zespołami testy, które były w rzeczywistości wykonywane zaledwie przez kilka godzin.

Ryzyko związane z testami penetracyjnymi i autoryzacja

Doświadczony zespół bezpieczeństwa ofensywnego powinien przeprowadzić dyskusję na temat zagrożeń związanych z ich działaniami i aktywnościami podczas trwania całej operacji. Zaleca się również z wyprzedzeniem zadać zainteresowanym stronom określony zestaw pytań, aby zrozumieć poziom dojrzałości grupy biznesowej lub celu, z którymi ma się do czynienia. Głównym celem przeprowadzania analizy ryzyka na tym etapie jest upewnienie się, że zespół bezpieczeństwa ofensywnego nie spowoduje przypadkowego przestoju, który można było przewidzieć.

Podczas tych rozmów mogą pojawić się np. następujące pytania.

- Czy na danym celu przeprowadzano już kiedykolwiek wcześniej testy penetracyjne?
- Czy zespół inżynierów przeprowadzał fuzzing?
- Ile jednoczesnych połączeń może obsłużyć system?
- Czy na liście celów znajdują się aktywa produkcyjne lub nieprodukcyjne?
- Czy system jest współdzielony przez wielu użytkowników, np. czy są to usługi w chmurze, czy też mamy do czynienia z hostingiem dedykowanym?

W zależności od dojrzałości systemu będącego celem ataku, różne zainteresowane strony mogą wyrazić swoją opinię i autoryzować operację. Zależy to od konkretnej działalności gospodarczej. Aby umożliwić skuteczne działanie zespołu bezpieczeństwa ofensywnego, warto, aby niektóre działania mogły być autoryzowane dość szybko, np. przez kierownika technicznego.

Organizacje bywają różne, kluczowe jest więc, żebyś wiedział, co działa dobrze w Twojej. Bywałem w organizacjach, które umożliwiały czerwonemu zespołowi swobodną pracę w sposób, jaki uważa za stosowny, pod warunkiem przestrzegania zasad przeprowadzania testów penetracyjnych i procedury SOP. W innych miejscach możesz spotkać się z tym, że szefowie działu bezpieczeństwa informacji oraz inni zainteresowani będą chcieli mieć większy wpływ na przeprowadzane testy.

Spotkanie wdrożeniowe

Jeśli czas i logistyka na to pozwalają, można zorganizować spotkanie wdrożeniowe ze wszystkimi zainteresowanymi stronami, aby różne zespoły i grupy mogły się zapoznać oraz ustanowić kanały komunikacji. Jest to ważne dla operacji fioletowego zespołu.

Rezultaty

Należy również ustalić, jakie będą oczekiwane rezultaty przed operacją, w jej trakcie i po zakończeniu. Obejmuje to potencjalne aktualizacje statusu, codzienne lub cotygodniowe spotkania informacyjne i optymalizacyjne, a także końcowe podsumowanie, raporty lub sprawozdania dla zainteresowanych stron.

Powiadamianie zainteresowanych stron

W zależności od rodzaju operacji do zainteresowanych stron wysyłane jest powiadomienie, które wskazuje zarys testu i jego cel, a także harmonogram. Powiadomienie powinno zawierać odniesienie do zasad przeprowadzania testów penetracyjnych i standardowej procedury operacyjnej. Może zostać wysłane do szerokiego grona odbiorców w celu zapewnienia przejrzystości operacji, ale może zostać również wysłane tylko do niezbędnych zainteresowanych stron, aby utajnić te operacje czerwonego zespołu, które mają na celu zweryfikowanie wysiłków w zakresie zapewnienia wewnętrznego bezpieczeństwa.

Powiadomienia mogą być przydatne na wiele sposobów. Po pierwsze, podnoszą świadomość kluczowych zainteresowanych stron na temat przeprowadzanych testów. W przypadku awarii lub zakłócenia świadczenia usług właściciel firmy może skontaktować się z zespołem testowym, aby zweryfikować, czy nie jest to przypadkiem związane z ich ofensywnymi działaniami w zakresie bezpieczeństwa. Po drugie, powiadomienia podnoszą ogólną świadomość zespołu w zakresie rodzaju przeprowadzanych testów.

Przykład możliwego powiadomienia pokazałem na rysunku 1.2.

W następnym punkcie tego podrozdziału dowiesz się, jak śledzić postęp podczas operacji.

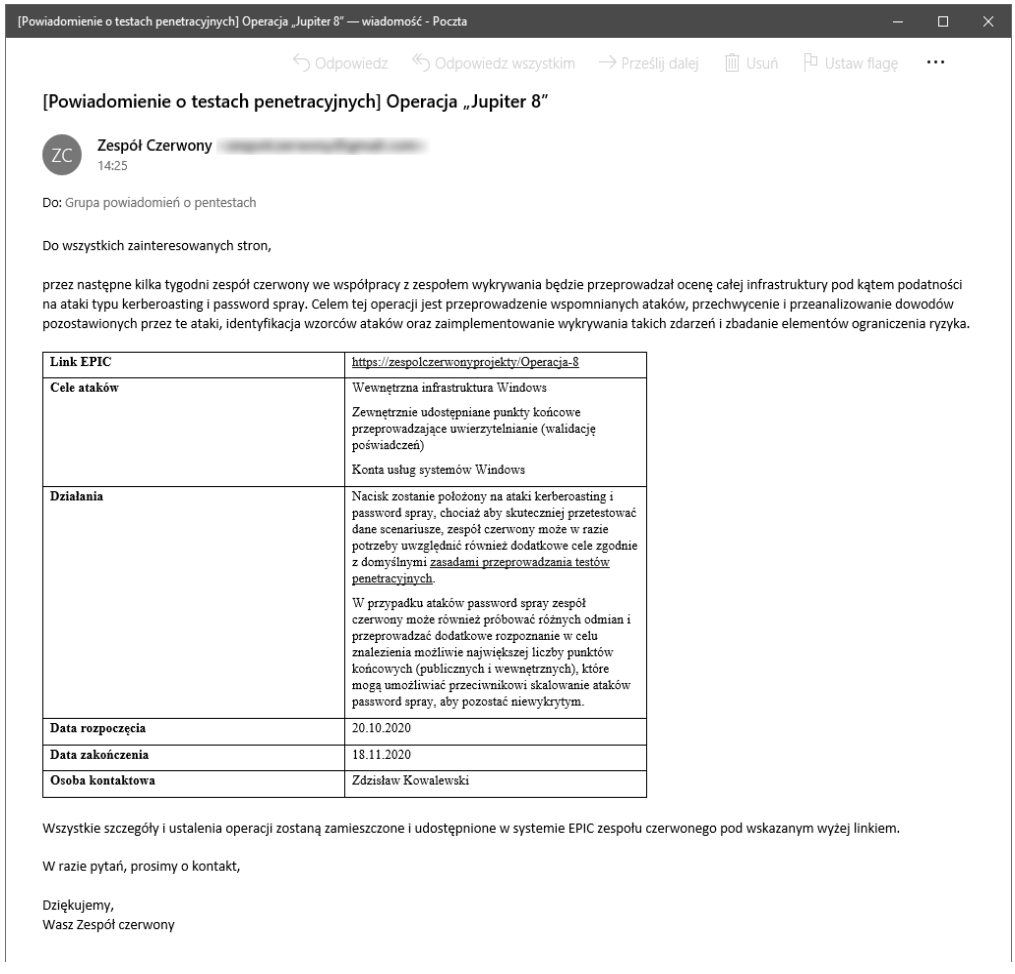
Wykonywanie planu ataku — śledzenie postępów w trakcie operacji

Może to być prosta lista zadań zapewniająca wykonanie wszystkich podstawowych testów podczas dokonywania ocen i przeprowadzania operacji. Najlepiej zdefiniować ją przed rozpoczęciem operacji, wskazując podstawowe cele i zadania, które należy wykonać.

Wartość posiadania takiego planu staje się oczywista podczas wykonywania większych, bardziej złożonych operacji z co najmniej czterema pentesterami i szeroką gamą celów. Plan ataku powinien być żywym dokumentem, co oznacza, że podczas każdej synchronizacji zespołu czerwonego, która powinna odbywać się regularnie, plan jest przeglądany, omawiane są postępy i dodawane nowe elementy (zadania) lub scenariusze do zbadania.

Ogromną zaletą jest również to, że ostatecznie łatwo zorientować się, które ścieżki nie zostały zbadane i należy do nich wrócić, uwzględniając je w przyszłym zleceniu. Takie informacje powinny zostać zawarte w sprawozdaniu.

Do przechowywania i śledzenia planów ataku można wykorzystać oprogramowanie, np. takie jak OneNote. Jeśli w swoich planach ataku będziesz przechowywać poufne informacje, zadbaj o to, żeby plan ataku był zaszyfrowany. Widziałem też, że zespoły w celu ułatwienia sobie współpracy wykorzystują instancje oprogramowania Mattermost (*https://www.mattermost.org/*) lub Slack.



[Powiadomienie o testach penetracyjnych] Operacja „Jupiter 8" — wiadomość - Poczta

Odpowiedz | Odpowiedz wszystkim | Prześlij dalej | Usuń | Ustaw flagę | ...

[Powiadomienie o testach penetracyjnych] Operacja „Jupiter 8"

ZC **Zespół Czerwony** [redacted]
14:25

Do: Grupa powiadomień o pentestach

Do wszystkich zainteresowanych stron,

przez następne kilka tygodni zespół czerwony we współpracy z zespołem wykrywania będzie przeprowadzał ocenę całej infrastruktury pod kątem podatności na ataki typu kerberoasting i password spray. Celem tej operacji jest przeprowadzenie wspomnianych ataków, przechwycenie i przeanalizowanie dowodów pozostawionych przez te ataki, identyfikacja wzorców ataków oraz zaimplementowanie wykrywania takich zdarzeń i zbadanie elementów ograniczenia ryzyka.

Link EPIC	https://zespolczerwonyprojekty/Operacja-8
Cele ataków	Wewnętrzna infrastruktura Windows Zewnętrznie udostępniane punkty końcowe przeprowadzające uwierzytelnianie (walidację poświadczeń) Konta usług systemów Windows
Działania	Nacisk zostanie położony na ataki kerberoasting i password spray, chociaż aby skuteczniej przetestować dane scenariusze, zespół czerwony może w razie potrzeby uwzględnić również dodatkowe cele zgodnie z domyślnymi zasadami przeprowadzania testów penetracyjnych. W przypadku ataków password spray zespół czerwony może również próbować różnych odmian i przeprowadzać dodatkowe rozpoznanie w celu znalezienia możliwie największej liczby punktów końcowych (publicznych i wewnętrznych), które mogą umożliwiać przeciwnikowi skalowanie ataków password spray, aby pozostać niewykrytym.
Data rozpoczęcia	20.10.2020
Data zakończenia	18.11.2020
Osoba kontaktowa	Zdzisław Kowalewski

Wszystkie szczegóły i ustalenia operacji zostaną zamieszczone i udostępnione w systemie EPIC zespołu czerwonego pod wskazanym wyżej linkiem.

W razie pytań, prosimy o kontakt,

Dziękujemy,
Wasz Zespół czerwony

Rysunek 1.2. Przykład powiadomienia o testach penetracyjnych

Pozostałe informacje, które można znaleźć w planie ataku, zostały omówione w kolejnych podpunktach.

Zadania i rezultaty rozpoznania

W tej sekcji wszyscy śledzą i zapisują spostrzeżenia dotyczące pracy białego wywiadu (ang. *open-source intelligence* — OSINT) i wyniki skanowania portów. Jeśli skanowanie jest w całości zautomatyzowane i dodatkowo śledzone wraz z upływem czasu, może to być link do bazy danych zawierającej te informacje lub dashboardu. Plan ataku można również postrzegać jako okazję do współpracy w zakresie sporządzania notatek i wskazywania ustaleń.

Scenariusze ataków

W tym miejscu zapisywane są scenariusze ataków prowadzące do osiągnięcia celów misji. Ta lista będzie w sposób naturalny wydłużać się podczas przeprowadzania operacji. Często zdarza się, że jednoczesne zastosowanie wielu exploitów umożliwia odegranie całego scenariusza. Czasami scenariusze ataków mogą zawierać różne pomysły do przemyślenia i zbadania, powstałe podczas intensywnej burzy mózgów.

Uwzględnianie wszystkich możliwych klas luk w zabezpieczeniach

Czy uwzględnione zostały wszystkie typowe klasy luk w zabezpieczeniach? Każdy pentester stosuje różne metody ataku, więc o ostatecznym sposobie przeprowadzania inspekcji kodu i aplikacji powinien decydować pentester. Najważniejsze, aby nie zniechęcać do eksplorowania nowych ścieżek wyszukiwania luk w zabezpieczeniach. Obszerne listy testów do wykonania dostępne są w doskonałych źródłach, takich jak podręcznik metodologii testów bezpieczeństwa (ang. *The Open Source Security Testing Methodology Manual* — OSSTMM) i fundacja OWASP (ang. *The Open Web Application Security Project*).

Zarządzanie błędami i incydentami

Ważne jest zdefiniowanie sposobu zarządzania błędami, w tym określenie, jak zespół pentesterów zamierza chronić poufne informacje przed operacją, w jej trakcie i po niej. Prawdopodobnie niezbędne będzie archiwizowanie ustaleń i dzienników testów penetracyjnych. Ponieważ ustalenia i dzienniki mogą zawierać poufne informacje, procedura SOP powinna określać kroki, które powinny zapewnić odpowiednią ich ochronę.

SOP może zawierać bardzo szczegółowe informacje na temat przepływu pracy oraz procesów i może się różnić w zależności od usług świadczonych przez zespół bezpieczeństwa ofensywnego.

Spotkania informacyjne i optymalizacyjne fioletowego zespołu

W zależności od rodzaju operacji procedura SOP może przewidywać obowiązkowe regularne spotkania informacyjne między zainteresowanymi stronami. W przypadku operacji fioletowego zespołu należy sformalizować organizowanie regularnych spotkań dla wszystkich kluczowych zainteresowanych stron, aby przeglądać wykonaną dotychczas pracę, dzielić się odkryciami oraz przeprowadzać burzę mózgów w celu wprowadzania usprawnień. Najlepiej, aby model operacyjny wyglądał w taki sposób, że zespół czerwony, zespół niebieski i niektórzy członkowie zespołu inżynierów znajdują się w tej samej lokalizacji, aby umożliwić stałą komunikację.

Dokumentowanie działań

Podczas zadań operacyjnych pentester powinien dokumentować co najmniej znaczące aktywności. Kolejne podpunkty zawierają kilka uwag i pomysłów dotyczących tego, co należy uwzględniać w dokumentacji i w jaki sposób to robić.

Zrzuty ekranu i dzienniki

Pentester powinien dokumentować przynajmniej znaczącą aktywność, co może polegać na wykonywaniu zrzutów ekranu i przechowywaniu dokładnego dziennika dostępu, zawierającego informacje o wykonanych działaniach oraz danych, do których uzyskano dostęp. Są to kluczowe informacje, które mogą być potrzebne do odróżnienia przyjaciela od wroga, a później do wprowadzania poprawek dotyczących luk w zabezpieczeniach i wyrzucania hakerów z systemu. Ponadto zespół niebieski może również weryfikować wykrycia i alerty bezpieczeństwa z dziennikami zespołu czerwonego.

Na koniec zespół bezpieczeństwa ofensywnego będzie chciał przedstawić „niezapomniane" sprawozdanie ze skutecznych działań, więc zrzuty ekranu z przeprowadzonej operacji oraz udokumentowane ustalenia są pomocne w zbudowaniu całej prezentacji.

Czasami zrzuty ekranu i dzienniki zawierają poufne informacje, więc należy pamiętać, że mogą wymagać specjalnego traktowania. Wiele standardowych narzędzi ma świetne możliwości rejestrowania, ale trzeba mieć świadomość, że zazwyczaj rejestrują one rzeczy w postaci zwykłego tekstu i należy zastosować dodatkowe szyfrowanie dzienników i danych. Jest to szczególnie ważne, jeśli raporty mają być archiwizowane przez dłuższy czas.

Nagrywanie ekranu

Niektóre elementy operacji powinny być nagrywane na wideo. Służy to celom edukacyjnym i jest wykorzystywane podczas zdawania sprawozdań w przypadku zakwestionowania działań zespołu. Ma to szczególnie ważne znaczenie podczas uzyskiwania dostępu do zasobów produkcyjnych. Chodzi o to, aby chronić pentestera na wypadek jakiegoś nieprzywidzianego zdarzenia albo w przypadku sporu o wykonane działania lub rodzaj informacji, do których uzyskano dostęp lub które zostały eksfiltrowane.

Testowanie w parach

Mówi się, że wielka władza wiąże się z wielką odpowiedzialnością. Gdy jest się inżynierem bezpieczeństwa ofensywnego, dość często ma się możliwość kontrolowania infrastruktury IT całych organizacji. Przy takich uprawnieniach zwykły błąd kliknięcia przycisku na klawiaturze lub myszy może doprowadzić do zakłócenia działania usługi lub usunięcia ogromnych ilości informacji. Aby uniknąć błędów i wypadków, zaleca się uruchamianie kluczowych części operacji w trybie parami oraz nagrywanie ekranu.

Czasami może to spowolnić jedną stronę, zwłaszcza jeśli młodszy pentester zostanie przydzielony do pary z kimś bardziej doświadczonym, ale jest to również świetna okazja do mentoringu i edukowania, aby pomóc rozwijać się jednostkom.

Podsumowywanie operacji

Po zakończeniu operacji należy sporządzić raport, podsumowanie lub sprawozdanie, aby upewnić się, że wszystkie zainteresowane strony otrzymają odpowiednie informacje.

Czyszczenie i archiwizowanie

W ramach podsumowywania operacji zespół bezpieczeństwa ofensywnego prawdopodobnie będzie musiał przeprowadzić pewne czynności porządkowe, takie jak czyszczenie środowisk ataków, usuwanie niepotrzebnej infrastruktury, która mogła zostać utworzona podczas operacji, a także archiwizowanie dzienników i planów ataków. W przypadku długoterminowej archiwizacji zalecam zaszyfrowanie tych artefaktów.

Wsparcie dla usuwania hakerów i naprawiania luk w zabezpieczeniach

Czasami czerwony zespół może zostać poproszony o pomoc w usuwaniu hakerów ze środowiska i naprawianiu znalezionych luk w zabezpieczeniach. Upewnianie się, że nie pozostały żadne niepotrzebne dodatkowe konta użytkowników jest najprawdopodobniej rolą pomocniczą. W zależności od zasad przeprowadzania testów penetracyjnych, czerwony zespół może z pewnością otrzymać pozwolenie (czasami nawet jest do tego zachęcany) na pozostanie w środowisku.

Jednym z obszarów, w którym zespół ofensywny również powinien służyć pomocą, jest edukacja użytkowników. Pentesterzy mogą np. powiadamiać osoby, których dane uwierzytelniające zostały skradzione, i przeprowadzać z nimi rozmowy. Powinni też informować te osoby o konieczności zmiany hasła i zachęcać do kontaktowania się, jeśli będą miały jakieś pytania. To praktyczne podejście oddolne jest bardzo skuteczne, a użytkownicy są bardzo zainteresowani tym, w jaki sposób włamano się do ich komputerów.

Raport i streszczenia

Jeśli zespół ofensywny jest dobrze zintegrowany z procesem inżynieryjnym i zarządzaniem incydentami, długi szczegółowy raport nie będzie potrzebny. Aby zwiększyć świadomość przeprowadzenia operacji i jej zakończenia, należy utworzyć dokument podsumowujący lub e-mail zawierający szczegółowe informacje o tym, co zostało zrobione i jakie osiągnięto rezultaty.

To streszczenie wskazuje problematyczne wzorce, najważniejsze ustalenia, a także to, co nie zostało przetestowane. Zawiera również odniesienia do szczegółowych informacji dotyczących konkretnych problemów. Te odniesienia to zwykle link do ustaleń, incydentów lub systemu śledzenia błędów. Moim zdaniem, problemy i incydenty powinny być śledzone bezpośrednio tam, gdzie pracują inżynierowie, niebieski zespół i respondery. Nie ma powodu, aby tworzyć kolejne miejsce do przechowywania poufnych informacji o szczegółach dotyczących luk w zabezpieczeniach.

Widziałem, że niektóre firmy śledzą wyniki testów penetracyjnych za pomocą innego systemu lub wprowadzają je do oddzielnego narzędzia do zarządzania ryzykiem, o którym większość

inżynierów nawet nie wie. Powoduje to, że inżynierowie nie poznają wyników testów penetracyjnych, dopóki nie wystąpi jakiś problem i — co nie powinno dziwić — w takich przypadkach problemy te nie są szybko usuwane.

Dokument *instruktażowy* reprezenuje tajne insformacje wymagające ochrony. Hakerzy mogą być szczególnie zainteresowani pozyskaniem tych raportów. Jeśli więc nie ma wyraźnego biznesowego powodu do tworzenia tak długich zbiorczych raportów, odradzam tę praktykę. Jest to jedna z różnic między wewnętrznym przeprowadzaniem operacji a zatrudnianiem zewnętrznego konsultanta do przeprowadzenia testów czarnej skrzynki. W takim przypadku możesz po prostu otrzymać pojedynczy raport, a następnie musisz samodzielnie opracować rozwiązanie i zastosować środki zaradcze.

Pamiętaj, że na tym etapie najlepiej byłoby, gdyby błędy zostały umieszczone w systemie śledzenia błędów.

Sprawozdanie

Spotkanie, na którym prezentowane jest sprawozdanie, to jeden z najważniejszych momentów, kiedy zespół bezpieczeństwa ofensywnego może wpływać na zmiany w organizacji i wskazywać, w jakim kierunku powinny podążać.

Sprawozdania będą prezentowane na sesjach wykonawczych, na których obecni będą właściciele firm, kierownictwo i kluczowe zainteresowane strony, które będą chciały uzyskać wszystkie informacje niezbędne do ustalenia właściwych kompromisów dotyczących ryzyka. Sprawozdanie może być również referowane szerszej publiczności, np. wszystkim inżynierom i członkom innych zespołów. To wszystko można wykonać w jednej sesji sprawozdawczej lub w wielu sesjach — często zależy to od preferencji Twojego klienta (wewnętrznego zespołu, z którym pracujesz). Osobiście uważam, że najlepiej zgromadzić podczas jednej sesji zarówno kadrę kierowniczą, jak i inżynierów, ponieważ mogą zostać przedyskutowane ważne kwestie. Dzięki temu do głosu mogą również dojść te strony, które często nie mają innej możliwości zaprezentowania swojego stanowiska.

Najlepszą praktyką podczas sesji sprawozdawczej jest wyświetlanie na ekranie koncepcyjnego grafu ataków, aby omówić etapy i rezultaty przeprowadzonej operacji. Graf może uwzględniać również ataki wykryte przez system bezpieczeństwa i ulepszenia wprowadzone w trakcie przeprowadzania operacji. Dalsza część sprawozdania powinna omawiać szczegółowo rezultaty, ale do zainicjowania dyskusji doskonale nadaje się przegląd konceptualny.

Na rysunku 1.3 przedstawiłem przykładowy graf ataków, który mógłby zostać zaprezentowany podczas sprawozdania. Pokazane są na nim najważniejsze ataki oraz wszelkie wykrycia, które miały miejsce. Aby przyciągnąć jak największą uwagę, uważam, że najlepiej prezentować graf za pomocą animacji krok po kroku, powoli ujawniając całą historię operacji.

Rysunek 1.3. Graf ataków ze sprawozdania podsumowującego

Sprawozdanie można wykorzystać również jako sesję edukacyjną lub szkoleniową, aby inne osoby w organizacji mogły uczyć się na błędach i ich nie powtarzać. Jeśli Twoja organizacja nie ma nic przeciwko temu, zespół ofensywny może również pomyśleć o przedstawieniu wyników na konferencji bezpieczeństwa.

Szczególną uwagę należy zwrócić na sprawozdania z operacji zespołu fioletowego. Działania zespołu czerwonego często tworzą wyłącznie obraz hakera, czasami w ogóle nie uwzględniając punktu widzenia zespołu niebieskiego. Sprawozdanie zespołu fioletowego koncentruje się na systemie wykrywania włamań i wprowadzonych ulepszeniach oraz próbuje wskazać obszary, które wymagają dalszych inwestycji.

Przemyślenia

Po każdej operacji wskazane jest omówienie tego, co poszło dobrze, a co można było zrobić lepiej. Może to obejmować działania na przyszłość oraz potencjalne pomysły na dalsze operacje, jeśli ocena niektórych aspektów systemu nie była możliwa z powodu ograniczeń czasowych lub zasobów.

Zespół może również określić swoje braki w przeszkoleniu lub wiedzy, które należy uzupełnić.

Uzyskanie sugestii i informacji zwrotnych od pozostałych zainteresowanych stron pozwoli również kierownikowi ocenić wyniki zespołu i udzielić indywidualnych wskazówek dotyczących tego, jak były postrzegane ich działania i komunikowanie się z zainteresowanymi stronami.

Aby zebrać opinie, zawsze na końcu każdego testu penetracyjnego chciałem utworzyć ankietę, którą mieliby okazję wypełnić wszyscy zaangażowani w cały proces. Niestety, w praktyce nigdy nie starczało czasu, aby dopracować szczegóły. Uważam jednak, że taka ankieta mogłaby dostarczyć ważnych obserwacji.

W przeszłości opracowałem ankietę na potrzeby szkoleń dotyczących bezpieczeństwa. Pomagała mi zrozumieć, w jaki sposób odbierani byli prelegenci, czy słuchaczom podobała się zawartość prezentacji, czy odnosiła się do ich pracy oraz jakie inne tematy mogą być interesujące na przyszłych szkoleniach.

Jestem przekonany, że zastosowanie tej samej metodologii zbierania informacji zwrotnych pod koniec testu penetracyjnego pomoże poprawić skuteczność programu bezpieczeństwa ofensywnego.

Udostępnianie nadrzędnych informacji za pośrednictwem dashboardów

Informacje, które obejmują wiele operacji, najlepiej udostępniać zainteresowanym stronom za pośrednictwem dashboardów. Więcej na temat pomiarów programu ofensywnego i stanu bezpieczeństwa organizacji przeczytasz w rozdziale 3., „Mierzenie efektywności programu bezpieczeństwa ofensywnego".

Kontaktowanie się z zespołem pentesterów i zamawianie usług

Jedną z rzeczy, których jeszcze nie omówiłem, jest sposób kontaktowania się osób z organizacji z zespołem testów penetracyjnych. Jeśli chce się robić postępy, trzeba mieć oczy i uszy szeroko otwarte. **Jak możemy zamówić przeprowadzenie testów peneteracyjnych w organizacji *xyz*?** Aby zapewnić oficjalny interfejs dla dowolnych osób z organizacji, wystarczy skonfigurować grupę e-mailową, taką jak *zamawanieczerwonegozespołu* lub coś w tym stylu. W ten sposób każdy ma bezpośredni kanał kontaktu z czerwonym zespołem i może poprosić o pomoc lub zasoby.

Bardziej dojrzałym sposobem jest utworzenie portalu lub systemu angażowania zespołu testów penetracyjnych, w którym ktoś może złożyć wniosek o świadczenie usługi za pośrednictwem prostego systemu biletów. W ten sposób znajdzie się on bezpośrednio w kolejce segregowania ważności zadań dla zespołu przeprowadzającego testy penetracyjne.

Procedura SOP powinna zawierać również pewne metadane, które ułatwią postęp konwersacji. Obejmuje to informacje o celu i zamawianej usłudze oraz przybliżone ramy czasowe.

Najlepszym sposobem śledzenia tych informacji jest użycie systemu zarządzania projektami, takiego jak Visual Studio lub Jira — wykorzystaj wszystko, co jest powszechnie używane w Twojej organizacji.

Modelowanie przeciwnika

Jednym z podstawowych obowiązków zespołu bezpieczeństwa ofensywnego jest strategiczne modelowanie przeciwników i zagrożeń, z którymi boryka się organizacja. Ten program powinien być bezpośrednio uwzględniany w procesie zarządzania ryzykiem. Na ogólnym poziomie można rozróżnić adwersarzy zewnętrznych i wewnętrznych, chociaż większość prawdopodobnych celów szkodliwych działań ma jakąś formę motywacji zewnętrznej. Wewnętrzny pracownik może być np. szantażowany przez agencję rządową w celu eksfiltracji rekordów z baz danych klientów. Mimo że jest to postrzegane jako klasyczne działanie wewnętrzne, rzeczywisty podmiot, który za tym stoi, jest zewnętrzny.

Zrozumienie przeciwników zewnętrznych

Jest to aktor lub zagrożenie, które pochodzą całkowicie spoza organizacji i działają poza nią. Do typowych przykładów należą tzw. skryptowy dzieciak (ang. *script kiddie*) lub agencja rządowa, którzy próbują przedostać się do wewnątrz organizacji. Taki przeciwnik będzie koncentrował się na powierzchni ataku danej organizacji, która obejmuje systemy i usługi udostępniane w internecie, a także fizyczne zagrożenia i fizyczne granice organizacji. Do zewnętrznych adwersarzy należą tacy „złośliwi aktorzy" (ang. *threat actor*) jak:

- skryptowe dzieciaki,
- haktywiści,
- przestępcy,
- szpiedzy,
- agencje rządowe.

Zazwyczaj ci aktorzy są klasyfikowani na podstawie wyrafinowania działania i zamiarów.

Uwzględnianie zagrożeń wewnętrznych

Kolejnym złośliwym aktorem jest osoba, która znajduje się już wewnątrz organizacji. Może to być np. niezadowolony pracownik, który szuka zemsty. Może się również zdarzyć, że jakiś pracownik będzie szantażowany, aby ukraść z organizacji kod źródłowy lub własność intelektualną (tak więc pracownik jest pośrednio celem jednego z zewnętrznych złośliwych aktorów opisanych wcześniej).

W typowej operacji zespołu czerwonego ten złośliwy aktor jest dobrym punktem zaczepienia, ponieważ należy założyć, że przeciwnik znajduje się już w granicach organizacji.

Inne zagrożenia wewnętrzne, które należy wziąć pod uwagę, to podstawowe błędy ludzkie lub wypadki, które mogą przydarzyć się podczas operacji.

Czynniki motywujące

Złośliwi aktorzy są motywowani określonym zestawem czynników. Zespół bezpieczeństwa ofensywnego analizuje i próbuje uwzględnić je, aby określić, jakie cele mogą interesować przeciwnika. Motywacje przeciwnika mogą być związane z czynnikami, takimi jak:

- zysk finansowy,
- zbieranie informacji wywiadowczych i szpiegostwo,
- hakowanie bez specjalnego celu, czyli tzw. hakowanie oportunistyczne,
- samospełnienie,
- badania i nauka,
- demonstracja siły.

Anatomia włamania

Do opisywania typowych działań podejmowanych przez przeciwnika podczas włamywania się do zasobów organizacji dostępny jest zestaw frameworków. Należy do nich np. dość popularny Lockheed Martin Kill-Chain (*https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf*).

Z biegiem lat powstały również bardziej wyrafinowane i ogólne frameworki, takie jak MITER ATT&CK (*https://attack.mitre.org*) lub Unified Kill Chain (*https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf*).

Łańcuch niszczenia intruzów (ang. *kill chain*) zdefiniowany przez Lockheeda Martina ma pewne ograniczenia i modeluje tylko pewien podzbiór przeciwników. Dalej w książce przeprowadzę bardziej dogłębną analizę i pokażę, jak te frameworki mogą pomóc w budowaniu strategii dla operacji i cyberobrony.

Nie sugerując się żadnym z tych konkretnych frameworków, omówię anatomię możliwego włamania, którego emulację jest w stanie przeprowadzić zespół czerwony.

Ustanowienie przyczółka

Początkowy punkt wejścia przeciwnika nazywa się **przyczółkiem** (ang. *beachhead*). Tego wojskowego terminu dla początkowego punktu wejścia włamania używa wiele zespołów ofensywnych. Termin przyczółek odnosi się do sytuacji, gdy żołnierze szturmujący plażę ustanawiają przyczółek, aby umożliwić linie wsparcia i zaopatrzenia. W terminologii bezpieczeństwa informacji przeciwnik wykorzystuje początkowo utworzony przyczółek do eksploracji otoczenia, otrzymywania wsparcia w postaci implantów, pivotowania do pobliskich obszarów i ruszenia do przodu w kierunku osiągnięcia celów misji.

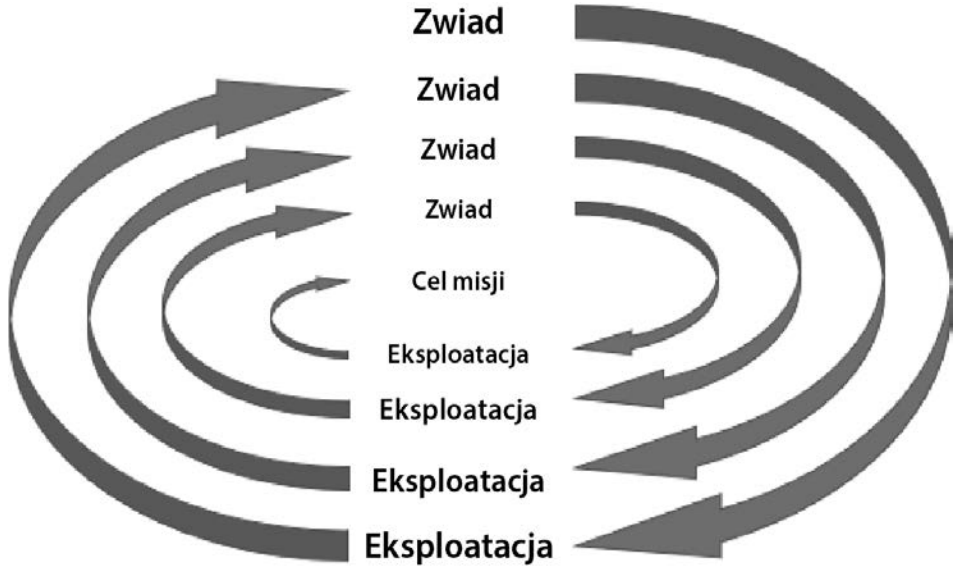
Dla obrońców możliwość prześledzenia wstecz i zidentyfikowania przyczółka jest kluczową umiejętnością, jaką powinni posiadać. Dojrzały zespół niebieski będzie miał wbudowaną automatyzację wstecznego śledzenia przeciwnika. Niestety, wiele organizacji nie ma wystarczających zasobów, umiejętności lub narzędzi, aby skutecznie, w rozsądnych ramach czasowych, odwrócić ścieżkę ataku obraną przez przeciwnika i znaleźć przyczółek. Obejmuje to takie przypadki jak usuwanie plików dziennika po długim okresie. Są to ustalenia, na które zwrócą uwagę operacje ofensywne.

Bez znalezienia punktu wejścia oraz załatania danej luki w zabezpieczeniach i jej wariantów każda próba pozbycia się hakera będzie skazana na niepowodzenie. Zespół czerwony ma za zadanie pomagać zespołowi niebieskiemu w rozwijaniu umiejętności niezbędnych do odnajdowania przyczółka i jego wszelkich możliwych wariantów.

Osiąganie celu misji

Typowy proces zdobywania celu lub wypełniania celu misji związany jest z dwiema podstawowymi fazami, czyli rozpoznaniem, po którym następuje eksploatacja. Potem rozpoczynana jest kolejna runda rozpoznania i eksploatacji z nowego punktu widzenia, co przybliża przeciwnika krok po kroku do celu. Czasami wystarczy tylko jedna pętla rozpoznania i eksploatacji, która prowadzi do bezpośredniej realizacji celu misji.

Uproszczony widok ataku przedstawiłem na rysunku 1.4.



Rysunek 1.4. Rozpoznanie i eksploatacja — pętla osiągania celu

Liczba cykli różni się w zależności od złożoności lub nasilenia ataku. Wstrzyknięcie SQL wymagałoby np. prawdopodobnie tylko jednej rundy lub dwóch, podczas gdy haker pivotujący przez infrastrukturę przed osiągnięciem celu mógłby wykonywać wiele cykli, w tym także podążać w złych kierunkach.

Włamywanie się do aplikacji internetowych

Wiele zasobów przeznacza się na działania czerwonego zespołu i śledzenie sieciowych ruchów bocznych wewnątrz organizacji i czasami wydaje się, że firmy nie robią wystarczająco dużo, aby chronić zewnętrzną powierzchnię ataku. Obejmuje to podstawowe luki w zabezpieczeniach na poziomie aplikacji, które umożliwiają przeciwnikowi bezpośrednie pobieranie danych klientów bez konieczności włamywania się w ogóle do wewnętrznej sieci korporacyjnej.

Wtedy może być tylko jeden cykl rozpoznania i eksploatacji!

Słabe poświadczenia

Żadna książka nie byłaby kompletna bez wskazania, że hasła są nieprawidłowe. Aplikacje i systemy internetowe z publicznym dostępem bez uwierzytelniania wieloskładnikowego nie zapewniają odpowiedniego poziomu ochrony. Temu ważnemu tematowi poświęcony został rozdział 7., „Polowanie na poświadczenia".

Brak integralności i poufności

Jaka jest pierwsza zasada większości agencji ochrony? Szukać zwykłego tekstu!

Jeśli chodzi o integralność i poufność, na przestrzeni lat poczyniono znaczne postępy. Technologie, takie jak TLS, są coraz szerzej stosowane w celu ochrony użytkowników. Narzędzia, takie jak FireSheep (*https://codebutler.com/2010/10/24/firesheep*), były niezwykle pomocne w zwiększaniu świadomości tego, co przeciwnik w kawiarni, w której korzysta się z publicznej sieci internetowej, może osiągnąć, wykorzystując niezabezpieczone protokoły.

Przed nami nadal długa droga. W zakresie integralności i poufności sytuacja wygląda dość źle, zwłaszcza gdy przeciwnik znajdzie się już w granicach korporacji. Wiele organizacji żyje w fałszywym przekonaniu, że (z jakiegoś magicznego powodu) komunikacja w intranecie lub w centrum danych jest zabezpieczona przed eksploatacją.

Łańcuch niszczenia intruzów Lockheeda Martina

We wstępie do tego podrozdziału wspomniałem o frameworku Lockheeda Martina służącym do modelowania włamań za pomocą łańcucha niszczenia intruzów (ang. *kill chain*). Na ten temat

dostępnych jest wiele dokumentacji i książek, więc nie będę powtarzał tutaj tego wszystkiego. Niektórym z tych pomysłów przyjrzymy się bliżej w rozdziale 3., „Mierzenie efektywności programu bezpieczeństwa ofensywnego". Na razie zajmę się raczej praktycznym przykładem tego, jak może wyglądać katastrofa usługi w chmurze.

Anatomia katastrofy usługi w chmurze

Przyjrzyjmy się typowemu scenariuszowi, w jaki sposób można się włamać do organizacji korzystającej z dostawcy usług w chmurze, takiego jak AWS, Google Cloud lub Microsoft Azure. Jest to przykładowy scenariusz, który pokazuje, jakie kroki może podjąć przeciwnik, i wskazuje wyjątkowe możliwości emulacji działań przeciwnika, jakie może zapewnić zespół bezpieczeństwa ofensywnego.

Na rysunku 1.5 pokazałem, w jaki sposób można się włamać do usługi w chmurze.

Rysunek 1.5. Graf ataku umożliwiającego włamanie się do usługi w chmurze

Jest to bardzo powszechny scenariusz ataków, który ma zastosowanie do większości organizacji. Przyjrzyjmy się szczegółowo różnym etapom przedstawionym na rysunku 1.5.

1. Początkowy krok przeciwnika (hakera) polega na utworzeniu ładunku w celu wysłania go do ofiary, która jest inżynierem DevOps, pracującym nad budowaniem i wdrażaniem głównego produktu wytwarzanego przez Twoją organizację.
2. Inżynier DevOps otrzymuje wiadomość e-mail i otwiera załącznik zawierający makro, które jest wykonywane i ustanawia przyczółek. Przeciwnik wykonuje teraz zrzut poświadczeń i *plądruje* maszynę w poszukiwaniu tajnych informacji, haseł i innych interesujących dokumentów. Szczęście mu sprzyja i odkrywa poświadczenia SSH lub Windows Remote Management do produkcyjnego serwera przesiadkowego (ang. *jump box*).
3. Korzystając ze skradzionych danych uwierzytelniających, przeciwnik pivotuje do produkcyjnego serwera przesiadkowego.

4. Gdy przeciwnik uruchomi złośliwy kod na produkcyjnym serwerze przesiadkowym, ponownie będzie szukać poświadczeń. Tym razem przeciwnik koncentruje się na znalezieniu plików *cookie*, które pozwolą mu zalogować się do konsoli zarządzania środowiskiem produkcyjnym dostawcy usług w chmurze.
5. Korzystając ze skradzionych plików *cookie*, przeciwnik wykonuje **atak Pass the Cookie** (dostarczanie plików *cookie* w sesji przeglądarki) w celu zalogowania się do konsoli zarządzania środowiskiem produkcyjnym.
6. W tym momencie przeciwnik ma pełny dostęp do wszystkich zasobów na danym koncie i jest gotowy do usunięcia lub zaszyfrowania wszystkich danych przechowywanych w systemach lub, co gorsza, może usunąć całą usługę w chmurze.

Tryby działania — operacja chirurgiczna lub nalot dywanowy

Podczas wykonywania operacji czerwonego zespołu istnieją dwa podstawowe podejścia do hakowania zasobów. Pierwsze jest bardzo ukierunkowane i chirurgiczne, a drugie to przeprowadzanie ewaluacji na dużą skalę i próby wykorzystania exploitów. Co zaskakujące, to drugie podejście często prowadzi do znacznie lepszego zrozumienia środowiska i odkrywania nieznanych obszarów. Omówię to nieco szerzej.

Działanie chirurgiczne

Operacja chirurgiczna wymaga zazwyczaj bardziej szczegółowego planowania i rozpoznania. Jest to dobre podejście, gdy w ramach operacji wyznaczane są jasne cele. Zadanie polega na pozostaniu niewykrytym przez całą operację. Podejście chirurgiczne mogłoby być np. tak bardzo ukierunkowane jak wysłanie wiadomości phishingowej do dwóch lub trzech osób i przejście do skrzynki odbiorczej ofiary w celu uzyskania dostępu do poufnych wiadomości e-mailowych lub kradzieży kluczowych informacji biznesowych z komputerów celu ataku.

Naloty dywanowe

Jest to rodzaj działania, które wykonuje zautomatyzowane złośliwe oprogramowanie (ang. *malware*). Zamiast wykonywać zrzuty poświadczeń na kilku wymaganych hostach, naloty dywanowe polegają np. na kradzieży poświadczeń w postaci zwykłego tekstu na każdym zasobie, na którym jest to możliwe.

Oczywiście, takie podejście jest hałaśliwe i bardziej prawdopodobne, że zostanie wykryte przez zespół niebieski. Jednak z drugiej strony podejście to uwydatni problemy i połączenia między systemami, które przed atakiem nie były widoczne dla nikogo w organizacji.

Posiadanie czerwonych zespołów, które przekraczają granice i wskazują nieznane dotąd zależności, ma ogromne znaczenie. Z mojego doświadczenia wynika, że zawsze dochodziło do co najmniej jednego odkrycia, które było całkowicie nieoczekiwane. Obejmowało np. znajdowanie danych uwierzytelniających kadry kierowniczej w miejscach, w których nikt by się ich nie spodziewał. Takie podejście może naturalnie niepokoić niektóre zainteresowane strony, ponieważ nie wiadomo, co zostanie odkryte, a zadaniem programu bezpieczeństwa ofensywnego jest podkreślanie kluczowego znaczenia takich postępowych technik.

To właśnie te nieznane obszary chcemy eksplorować i pokazać je kierownictwu i organizacji.

Środowisko i przestrzeń biurowa

Być może zastanawiasz się, dlaczego poświęciłem dodatkowy podrozdział środowisku pracy i przestrzeni biurowej. Przekonałem się, że jest to niezwykle istotny aspekt bezpieczeństwa dotyczący całej branży, zwłaszcza inżynierów oprogramowania. Wielu z nas pracuje teraz w otwartych biurach i wspólnych środowiskach.

Obecnie każdy lubi otwarte biura — przynajmniej tak wmawia nam kierownictwo. Zamiast zagłębiać się w to, co oznacza to dla programistów, którzy zajmują się również poufnymi informacjami i własnością intelektualną, napiszę, co oznacza to dla inżynierów bezpieczeństwa, szczególnie tych, którzy mają do czynienia z hasłami systemów i innych pracowników w postaci zwykłego tekstu, a także z potencjalnymi informacjami o niezałatanych lukach w zabezpieczeniach itd.

Porównanie otwartej i zamkniętej przestrzeni biurowej

Osobiście nie jestem wielkim zwolennikiem otwartych biur, chociaż w przypadku testów penetracyjnych otwarte biuro zaskakująco dobrze się sprawdza, z jednym zastrzeżeniem: upewnij się, że w sąsiedztwie masz tylko pentesterów!

Dzieje się tak głównie z dwóch powodów: po pierwsze, chcesz, aby zespół mógł swobodnie mówić i dzielić się pomysłami, co może obejmować udostępnianie poufnych informacji, a po drugie, wiele testów penetracyjnych to praca zespołowa, dzielenie się pomysłami, omawianie postępów oraz wtrącanie swoich trzech groszy, aby pomóc innym.

Zabezpieczenie środowiska fizycznego

Nawet jeśli kierownictwo może dążyć do przejścia na układ otwartego biura lub już do tego doprowadziło, ponieważ wszyscy inni też tak robią, ważne jest zapewnienie przynajmniej Twojemu zespołowi specjalnego środowiska fizycznego, które można zamknąć, aby dostęp do niego miały tylko zainteresowane strony z dobrym powodem biznesowym.

Poczucie bezpieczeństwa i możliwość swobodnego komunikowania się i dzielenia pomysłami, atakami itd. ma kluczowe znaczenie podczas operacji.

Jeśli trzeba, zbieraj najlepsze zespoły

Jeśli wszyscy Twoi pentesterzy mają własne biura, warto wypróbować montowanie zespołów. Do następnej operacji zbierz np. specjalną grupę zadaniową i poproś, aby pracowali we wspólnej przestrzeni. Wystarczy znalezienie oddzielnego pomieszczenia, w którym zespół będzie pracował podczas operacji. To podejście zapewniło mi najwięcej radości i sukcesów podczas przeprowadzania testów penetracyjnych. Jeżeli wcześniej nie robiłeś czegoś takiego, warto wypróbować wady i zalety tego podejścia.

Skoncentrowanie się na aktualnym zadaniu

Podczas operacji pentester będzie miał do czynienia z poświadczeniami w postaci zwykłego tekstu i będzie pracował z exploitami, starając się osiągnąć cele misji. Kierownik musi zapewnić zespołowi możliwość skupienia się i niezakłóconej pracy w kluczowych momentach. Nie ma nic bardziej przeszkadzającego i prawdopodobnie niebezpiecznego, niż hakowanie kontrolera domeny podczas rozmowy z kimś na temat tego, kiedy zostanie sprawdzony błąd zgłoszony trzy miesiące temu.

Podsumowanie

W tym rozdziale przeanalizowałem podstawy budowania skutecznego programu testów penetracyjnych w organizacji. Obejmuje to sposoby wpływania na kierownictwo w celu wspierania programu bezpieczeństwa ofensywnego i definiowanie jasnej misji, aby inicjować działania. Omówiłem usługi, jakie czerwony zespół może świadczyć organizacji, i wyjaśniłem, co jest potrzebne do ustanowienia programu bezpieczeństwa ofensywnego w organizacji.

Aby działać pewnie i bezpiecznie, położyłem nacisk na tworzenie zasad przeprowadzania testów penetracyjnych i procedur SOP.

Ponadto wyjaśniłem, z jakiego rodzaju przeciwnikami mogą borykać się organizacje i jak dochodzi do włamań do systemów. Podałem także kilka wskazówek, jak przekazać te informacje pozostałym zainteresowanym stronom.

W następnym rozdziale dowiesz się, jak zarządzać czerwonym zespołem i rozwijać go, oraz jak dalej rozwijać ogólny program, aby poprawić jego dojrzałość.

Pytania

1. Wymień co najmniej dwa powody dla ustanowienia programu czerwonego zespołu.
2. Jakie usługi może zapewnić organizacji wewnętrzny program bezpieczeństwa ofensywnego?
3. Jakie są zasady przeprowadzania testów penetracyjnych i dlaczego tak ważne jest ich ustalenie?
4. Wymień co najmniej trzech zewnętrznych przeciwników, z którymi Twoja organizacja może mieć do czynienia.

Wróg nie śpi. Przejdź do ofensywy i testuj swój system!

Zapewnienie bezpieczeństwa IT jest wyjątkowo ważne. Organizacja musi pozostawać w ciągłej gotowości do wykrywania zagrożeń i reagowania na incydenty bezpieczeństwa. Przeciwnicy nieustannie się doskonalą i standardowy zestaw zabezpieczeń jakiś czas temu przestał wystarczać. Konieczne jest zbudowanie i wdrożenie kompleksowego systemu zapobiegania zagrożeniom, ich wykrywania i reagowania na nie. Podobnie jak na polu bitwy, tak i w planowaniu bezpieczeństwa IT zyskuje się przewagę dzięki znajomości własnego terenu i działaniom ofensywnym.

Oto wszechstronny i praktyczny przewodnik dla inżynierów i kierowników do spraw bezpieczeństwa. Opisano w nim, jak zbudować program pracy zespołu czerwonego, który będzie się zajmować ofensywnymi testami bezpieczeństwa, zarządzać nim i monitorować ich efektywność. Omówiono też skuteczne sposoby podnoszenia świadomości bezpieczeństwa w organizacji. Dokładnie wyjaśniono zasady wykonywania operacji progresywnych, takich jak ukierunkowane testy naruszenia prywatności czy manipulowanie danymi telemetrycznymi. Zaprezentowano grafy wiedzy i sposoby ich budowania, a następnie techniki polowania na poświadczenia. Nie zabrakło ważnych uwag o ochronie zasobów, przeprowadzaniu audytów oraz korzystaniu z alertów.

W książce:

- czym grożą naruszenia bezpieczeństwa
- jak budować skuteczne zespoły testów penetracyjnych
- mapowanie własnego terenu za pomocą grafów wiedzy
- czym jest polowanie na poświadczenia
- czym się różni praca zespołów niebieskiego i czerwonego
- skuteczne informowanie kierownictwa firmy o problemach z bezpieczeństwem

Johann Rehberger — od kilkunastu lat zajmuje się analizą i modelowaniem zagrożeń, zarządzaniem ryzykiem, testami penetracyjnymi oraz ofensywnymi testami bezpieczeństwa. Był instruktorem etycznego hakowania na Uniwersytecie Waszyngtońskim. Przez wiele lat zajmował się bezpieczeństwem w Microsofcie i Uberze, obecnie jest niezależnym ekspertem.

ISBN 978-83-283-7404-1
9 788328 374041
Cena: 99,00 zł

Packt