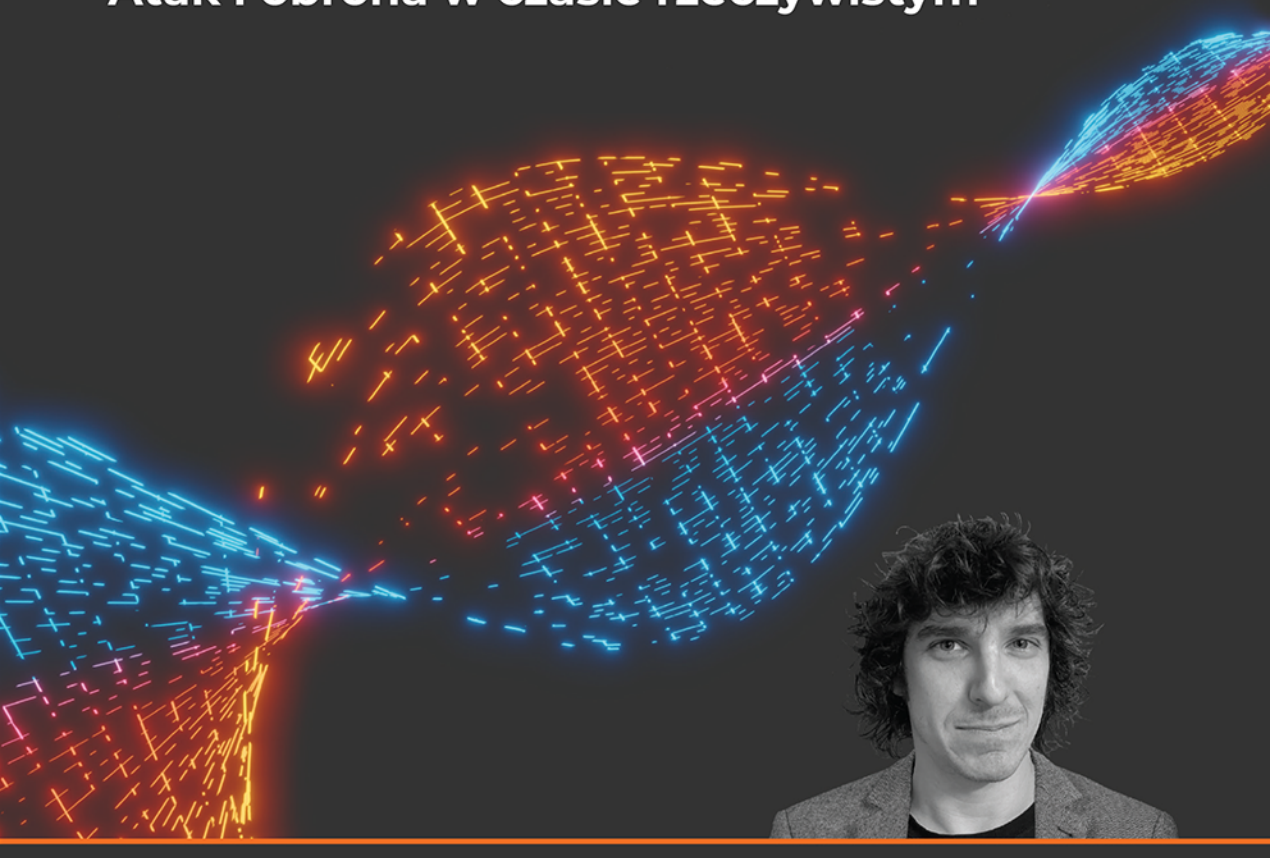
Wydanie II

Sztuka prowadzenia cyberkonfliktu

Atak i obrona w czasie rzeczywistym



Dan Borges

Helion
Packt

Tytuł oryginału: Adversarial Tradecraft in Cybersecurity:
Offense versus defense in real-time computer conflict

Tłumaczenie: Aleksander Łapuć

ISBN: 978-83-283-8684-6

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

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
https://ftp.helion.pl/przyklady/cybkon.zip

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

Printed in Poland.

Spis treści

2

ROZDZIAŁ

Przygotowanie do bitwy

W tym rozdziale przedstawię, jakie przygotowania są niezbędne przed rozpoczęciem trudnego i wymagającego cyberkonfliktu. W poprzednim rozdziale wspominałem, że w każdym zaawansowanym działaniu *zasada planowania* odgrywa kluczową rolę, zwłaszcza w konkursach opartych na rywalizacji. Cytując Benjamina Franklina: „Porażka podczas przygotowań to przygotowanie do porażki". Stwierdzenie to zachowuje pełną słuszność także w przypadku konfliktów komputerowych. Aby skutecznie użyć narzędzi i infrastruktury, niezbędne jest posiadanie odpowiednich kompetencji, a te można zdobyć jedynie inwestując znaczną ilość czasu i wysiłku w naukę. Zajmę się teraz krokami przygotowawczymi, które każda ze stron cyberkonfliktu powinna podjąć, zanim rozpocznie działania operacyjne. Pokażę różnice pomiędzy długofalowym planowaniem strategicznym a krótkoterminowym planowaniem operacyjnym. Zaprezentuję, jak można podzielić długofalowe planowanie na mniejsze komponenty, jakich miar używać do oceny planów strategicznych oraz jak ocenić efektywność operacyjną. Celem planowania jest przygotowanie skutecznego planu, stworzenie dokumentacji w formie stron wiki, zdefiniowanie procesów operacyjnych, a nawet zaprogramowanie automatyzacji wybranych strategii, aby zapewnić spójność i powtarzalność ich użycia. Przeanalizuję, jakie umiejętności i jakie elementy infrastruktury powinny być objęte planowaniem — zarówno z perspektywy ataku, jak i obrony. W treści rozdziału zaprezentuję liczne opcje technologiczne i rozwiązania — część już pewnie będzie Ci znana, ale mam nadzieję, że poznasz też wiele nowych. Należy dążyć do uproszczenia wielkoskalowych działań w obszarze bezpieczeństwa komputerowego poprzez odpowiednie ich zaplanowanie oraz wykorzystanie platform programistycznych wspomagających automatyzację i zarządzanie niezbędnymi do wykonania zadaniami. Przygotowywane plany muszą cechować się elastycznością, z punktu widzenia zarówno zespołu wdrożeniowego, jak i operacyjnego. Trafnie ujął to Eisenhower: „Plany są bezużyteczne, ale planowanie jest nieodzowne". Oznacza to, że konkretne kroki, jakie będą podejmowane w trakcie działań, mogą odbiegać od wcześniej ustalonego planu. Zatem plan nie powinien być traktowany jako dogmat, lecz raczej jako ogólna mapa wytyczająca drogę do celu — szczególnie przydatna w momentach stresujących lub kryzysowych.

W dalszej części rozdziału omówię następujące tematy:

- komunikacja,
- metody budowania zespołu,
- planowanie długofalowe,
- planowanie operacyjne,
- zbieranie danych,
- zarządzanie danymi po stronie obrony,
- analiza danych po stronie obrony,
- stosowanie wskaźników wydajności po stronie obrony,
- zbieranie danych po stronie ataku,
- wytwarzanie narzędzi ofensywnych,
- stosowanie wskaźników wydajności po stronie ataku.

Podstawowe rozważania

Rozpocznę od kilku schematów i rozwiązań, które możesz wykorzystać w planach swojego zespołu, czy to szykując się do konkursów bezpieczeństwa, czy przygotowując większą operację w rzeczywistości. Podstawowe kwestie są wspólne dla obu stron konfliktu. Powodzenie operacji ataku i obrony zależy od ustanowienia bezproblemowej komunikacji i od współdzielenia informacji. Obie strony konfliktu muszą stworzyć i utrzymać zespół, który będzie tę operację prowadził. I obie strony muszą przeprowadzić procesy planowania strategicznego i operacyjnego. W tym podrozdziale skupiam się na elementach wspólnych dla ataku i obrony, a w kolejnych zajmę się różnicami pomiędzy tymi zespołami.

Komunikacja

Tworzenie zespołu operacyjnego należy zacząć od udokumentowania ogólnych planów działania, aby mieć pewność, że zostały wyznaczone ogólne cele oraz że istnieje co najmniej wspólne rozumienie kierunku, w którym będzie się rozwijać działalność operacyjna. Zapisana postać tych planów będzie przydatna przez dłuższy czas, gdyż tworzenie kolejnych planów, współpraca w ramach zespołu oraz rozwój zespołu muszą odbywać się w odniesieniu do tych pierwszych, najważniejszych planów strategicznych. Planowanie jest często postrzegane jako zadanie wyłącznie dla menedżerów, ale zwykli członkowie zespołu mogą zyskać na uczestnictwie w procesie planowania. Wspólne planowanie przedsięwzięcia jednoczy zespół wokół wspólnej wizji. Uruchomienie serwisu wiki do przechowywania i współdzielenia wiedzy w zespole będzie wielką korzyścią zarówno dla zespołu atakującego, jak i dla zespołu broniącego — dzięki temu wiedza będzie mogła być kumulowana przez dłuższy czas poprzez zaangażowanie poszczególnych członków. Bazę wiedzy może także stanowić repozytorium kodu, takie jak GitLab, lub proste repozytorium dokumentów, takie jak dzielony dysk sieciowy. Ważne jest, by wybrane repozytorium było dostępne dla wszystkich członków zespołu — zależnie od potrzeb

może ono być uruchomione na publicznie dostępnym serwerze, w prywatnej sieci lub nawet jako wciąż zmieniająca położenie usługa sieci Tor. Bez względu na wybraną technologię repozytorium powinno stanowić wspólne medium, poprzez które członkowie zespołu dzielą się planami, narzędziami i informacjami na temat narzędzi, technik i polityk. Wybrane rozwiązanie powinno być w miarę trwałe, aby umożliwić długofalowe wsparcie zespołu. Wybór właściwego narzędzia do tworzenia dokumentacji wiki lub udostępniania repozytorium notatek jest kluczowy. Możesz zdecydować się na produkt instalowany na publicznie dostępnym serwerze wraz z interfejsem API umożliwiającym automatyczną integrację. Możesz wybrać rozwiązanie umieszczone w sieci prywatnej. Możesz też zamiast gotowego produktu wybrać rozwiązanie open source, dzięki czemu możesz zweryfikować jego kod źródłowy. Decyzja zależy od Twojej tolerancji ryzyka oraz ewentualnych wymagań dotyczących *poufności*. Możesz potrzebować rozbudowanych funkcjonalności *autoryzacji*, aby ograniczać dostęp do stron i obszarów roboczych pomiędzy użytkownikami lub grupami użytkowników. Rozdzielenie różnorodnych treści dotyczących wytwarzanych narzędzi lub szczegółów operacyjnych pozwala zmniejszyć niekorzystne skutki włamania na konto jednego z operatorów. Osobiście bardzo cenię możliwość jednoczesnej grupowej edycji dokumentów, dostępną na przykład w Google Docs lub Etherpad[1] — jest ona niezwykle przydatna, gdy rozproszony zespół edytuje i przegląda dokumenty w czasie rzeczywistym. Kolejną istotną funkcjonalnością może być możliwość wysyłania powiadomień oraz informowania o zmianach poprzez e-mail. DokuWiki jest dobrym przykładem aplikacji wiki, którą można zainstalować w obrębie własnej infrastruktury. Jest prosta, jej kod źródłowy jest publicznie dostępny i używałem jej przy różnych okazjach[2]. Rozważaliśmy różne funkcjonalności i opcje, jakie może posiadać rozwiązanie wiki, ale w kontekście konkursów wybór powinien być prosty. Należy wybrać proste, łatwo dostępne rozwiązanie, zapewniające metody *uwierzytelniania* i *poufność* dostępu do zawartości, a także sprzyjające współpracy grupowej.

Technologie do komunikacji w czasie rzeczywistym, w szczególności czaty, są niemal tak samo ważne jak rozwiązania do współdzielenia wiedzy. Komunikacja jest siłą napędową każdego zespołu. Im szybciej następuje komunikacja między członkami zespołu, tym szybciej członkowie mogą wymieniać, opracowywać i rozwijać wspólne pomysły. Możliwość komunikacji z użyciem czatu jest kluczowa dla powodzenia zespołu, więc ważne jest, by wybrać odpowiednią infrastrukturę lub dobrze wykorzystać dostępną. Nawet jeżeli Twój zespół jest w tak luksusowej sytuacji, że wszyscy przebywają w tym samym pomieszczeniu, to i tak będą musieli przesyłać między sobą cyfrowe treści, takie jak pliki i zawartości dzienników zdarzeń. Zazwyczaj wybrane narzędzie komunikacyjne powinno być główną metodą dla cyfrowych interakcji w obrębie zespołu — może to być e-mail, IRC, XMPP, Slack, Mattermost, Zoom czy nawet bardziej ulotna komunikacja poprzez Etherpad. Ważną cechą, którą należy wziąć pod uwagę przy wyborze narzędzia, jest możliwość kopiowania i wklejania treści bezpośrednio w ramach obszaru operacyjnego — dlatego na przykład komunikacja oparta na wiadomościach SMS może nie sprawdzić się jako główna forma kontaktu. Możesz też rozważyć pójście o krok dalej i wyposażyć swój czat grupowy w dodatkowe opcje, pozwalające między innymi zintegrować czat z różnymi narzędziami operacyjnymi i zarządczymi, czyli zamienić go w *chat-ops*. Dzięki funkcji tworzenia zadań grupowych bezpośrednio z poziomu czatu Twój zespół zyskuje potężne możliwości automatyzacji, na przykład możliwość wykonywania publicznej oceny hostów lub odbierania wyników skanowania sieci i przekazywania ich całemu zespołowi w obrębie czatu grupowego. W przeszłości używałem rozwiązania *chat-ops* wraz z zespołem reagowania na

incydenty bezpieczeństwa. Mogliśmy bardzo szybko i z udziałem całego zespołu przebadać wszystkie pracujące w naszym środowisku maszyny w poszukiwaniu konkretnych wskaźników włamania. Mogliśmy z poziomu czatu zlecać pobranie wybranych artefaktów z komputerów oraz przestawiać maszyny w tryb kwarantanny, więc w trakcie oceny rozmiaru incydentu mogliśmy bardzo szybko dokonać oceny maszyn i osiągnąć niskie czasy reakcji. Jeżeli zdecydujesz się na intensywne wykorzystanie podejścia *chat-ops*, to koniecznie załóż oddzielne pokoje konwersacyjne w tym celu, bo wiadomości przesyłane przez automaty mogą czasem całkowicie wyprzeć komunikaty od ludzi. Kolejną funkcjonalnością wartą rozważenia jest możliwość szyfrowania zapisanej historii czatów, dzięki czemu komunikacja w zespole ma zapewniony dodatkowy poziom *poufności* i *integralności*. W aplikacji Slack jest dostępna płatna opcja wspierająca szyfrowanie: Enterprise Key Management (EKM). Funkcjonalność EKM umożliwia szyfrowanie wiadomości i dzienników zdarzeń za pomocą własnych kluczy kryptograficznych przechowywanych w usłudze Amazon Key Management Service (AWS KMS)[3]. Te funkcjonalności mogą być prawdziwym wybawieniem, jeżeli do części Twojej organizacji lub infrastruktury nastąpi włamanie, pozwalają bowiem oddzielnie szyfrować historię różnych pokoi konwersacyjnych i dzienników zdarzeń. Dobrze jest także mieć zapasowe rozwiązanie komunikacyjne na wypadek, gdyby do głównej aplikacji czatu nastąpiło włamanie lub z innego powodu utracona została jej *dostępność*. Czat zapasowy powinien wykorzystywać silną kryptograficzną metodę *uwierzytelniania*, na przykład za pomocą kluczy GPG lub z użyciem takich rozwiązań jak Signal[4]. Dzięki systemowi współdzielenia wiedzy i systemowi efektywnej komunikacji zespoły będą mogły wydajnie współpracować nad tworzeniem planów i dalszym rozwojem używanej infrastruktury. Oba komponenty są kluczowe zarówno dla zespołu ataku, jak i obrony.

Planowanie długofalowe

Planowanie długofalowe jest jednym z najistotniejszych typów planowania, jakimi może się zająć Twój zespół. W ten sposób możecie ustalić myśl przewodnią dla zespołu oraz określić nadrzędny kierunek działań i metodę wyrażania innowacyjnych pomysłów. Ile konkretnie czasu oznacza długofalowość, zależy od zakresu prowadzonych operacji. W przypadku konkursów może to oznaczać planowanie w cyklach rocznych albo planowanie obejmujące tylko kilka tygodni przed wydarzeniem. Ogólnie rzecz ujmując, planowaniem należy objąć taki okres, aby w okresie spokoju dobrze przygotować się do wykonania operacji. Możesz także sukcesywnie modyfikować stworzone plany, w miarę jak działania operacyjne się rozwijają i rozpoznawane są nowe potrzeby — na przykład przez dodawanie lub usuwanie kamieni milowych. Przykładami planowania długofalowego są plany obejmujące od trzech do pięciu lat, plany roczne, plany kwartalne, plany miesięczne, a czasem nawet przygotowanie do pojedynczego wydarzenia konkursowego — w takim przypadku planowanie mogłoby obejmować szkolenia poświęcone zakresowi tego wydarzenia oraz przygotowanie do aktywnego wyszukiwania zagrożeń bezpieczeństwa. Planowanie wysokopoziomowe może wydawać się błahe, ale dobrze jest, by zespół miał ogólne rozumienie wyznaczonego nadrzędnego kierunku działań. Najlepiej jest taki plan zapisać, aby mieć pewność, że wszyscy są co do niego zgodni.

Z czasem ogólne plany mogą zostać podzielone na cele pośrednie, dzięki czemu poszczególne inicjatywy będą bardziej strawne dla zespołu, a konkretne zadania będzie łatwiej umieścić w ramach czasowych. Takie kamienie milowe pomagają ustalić, czy uzyskane postępy są zgodne

z pierwotnym planem i harmonogramem. Czas jest jednym z najcenniejszych zasobów, jakimi dysponujesz, dlatego planując z wyprzedzeniem, możesz łatwiej uporać się z większymi zadaniami i pochłaniaczami czasu. Wykorzystaj okresy spokoju pomiędzy operacjami do wytwarzania narzędzi i implementowania automatyzacji, które przyspieszą Twoje działania. Na przykład jeżeli zespół spędza znacząco dużo czasu na kontroli uprawnień dostępowych użytkowników i realizacji procedur zmiany lub odblokowania hasła, to warto zaplanować wytworzenie narzędzi wspierających te zadania. Planowanie długofalowe powinno obejmować inicjowanie projektów, w ramach których zostaną wytworzone potrzebne elementy infrastruktury i narzędzia udostępniane zespołowi lub zostaną przeprowadzone szkolenia podnoszące poziom umiejętności członków zespołu. Upewnij się, że planujesz czas trwania projektów i okresy pomiędzy kamieniami milowymi z odpowiednimi zapasami, na wypadek dodatkowych prac wymaganych do naprawy błędów. Dlatego też nie należy przypisywać zbyt wielu równolegle trwających zadań jednej osobie ani planować wykonania zbyt wielu projektów naraz. W wyniku planowania długofalowego możliwości Twojego zespołu będą wzrastać przez dłuższy czas, więc nie staraj się za bardzo pośpieszać wykonywania bieżących projektów, aby nie wypalić przedwcześnie sił zespołu. Z drugiej strony, jeżeli planowanie długofalowe okaże się zupełnym fiaskiem, może się okazać, że wejdziesz w cyberkonflikt bez odpowiedniego przygotowania technicznego, miotając się w próbach zbudowania jakichkolwiek narzędzi, a nawet pozostając kompletnie ślepym na działania przeciwnika.

Żaden plan nie jest doskonały. Potrzebujesz metod pomiaru stopnia, w jakim udało się zrealizować stawiane cele, aby dokonywać potrzebnych korekt w razie rozbieżności z planem. Stwórz plany naprawcze na wypadek, gdyby cele, kamienie milowe lub oczekiwane wartości wskaźników pomiarowych nie zostały osiągnięte. Ten temat zasygnalizowałem podczas omawiania *zasady planowania*, a rozwinę go w tym rozdziale. Przez całą treść książki będę poszukiwał metod pomiaru parametrów i weryfikacji stosowanych technik, pozwalających upewniać się, czy wszystko toczy się zgodnie z planem i harmonogramem. Odpowiedni wybór momentu realizacji planów jest krytycznie ważny w trakcie prowadzenia działań wobec przeciwnika, aby przełączając się między planami, utrzymać przewagę — wspomniałem o tym, opisując *zasadę czasu*. Jeżeli zbierane w trakcie operacji dane są niezgodne z przewidywanymi przez realizowany plan, na przykład wykryte zostało użycie pewnych niespodziewanych technik, to konieczna jest modyfikacja planów, być może też narzędzi, aby zastosować odpowiednie nowe strategie. Jest to istota *zasady innowacji*: jeżeli używana strategia zostanie ujawniona przez przeciwnika, to utracimy przewagę, więc należy być przygotowanym do zmiany sposobu prowadzenia operacji w takim momencie. Były mistrz mieszanych sztuk walki Georges St-Pierre powiedział: „Innowacja jest dla mnie bardzo ważna, zwłaszcza zawodowo. Odmienne podejście, czyli uporczywe trwanie przy tym samym, prowadzi do samozadowolenia, braku elastyczności i w konsekwencji do porażki. Dla mnie innowacja oznacza postęp, wprowadzanie do moich działań nowych elementów i modyfikowanie istniejących”[5]. W trakcie przygotowywania planów długofalowych zastanów się nad zarezerwowaniem czasu na przeprowadzenie nieokreślonych początkowo badań, wytworzenie nieznanych jeszcze narzędzi lub udoskonalenie procesów. Dzięki umieszczeniu w planach długofalowych takich bloków aktywności, początkowo nie wypełnionych konkretnymi zadaniami, będziesz mieć możliwość łatwiejszego wprowadzania zmian w przyszłości — jeżeli realizacja planu znacząco odbiegnie od zakładanego przebiegu, będzie można poświęcić te bloki, by skorygować kurs. A jeżeli plan będzie wykonywany bez

przeszkód, to w ramach czasu przewidzianego na te bloki będzie można przeprowadzić usprawnienia wykorzystywanych procesów.

Kompetencje

Wiedza jest jedną z najważniejszych rzeczy, jakie możesz przygotować. Podczas rekrutacji zwracaj uwagę na doświadczenie i talent, ale także na zamiłowanie do tematyki cyberbezpieczeństwa oraz dopasowanie do reszty zespołu. Lepiej budować doborowy zespół z członków wyselekcjonowanych pod względem kompetencji, doświadczenia i zdolności niż po prostu zarzucać problemy masą ludzką. Jednym z unikalnych aspektów informatyki jest możliwość automatyzowania rozwiązań i skalowania ich w górę. Oznacza to, że innowacyjny inżynier może zautomatyzować zadanie lub jego część, zastępując ręczną pracę kilku osób. To jednak nie zmienia faktu, że będziesz potrzebować zespołu. Po prostu istnieje bardzo wiele obszarów wiedzy i elementów skomplikowanej infrastruktury, więc nie da się zarządzać nimi zbyt małą liczbą osób. W planach długofalowych do każdego z obszarów eksperckich powinien być przypisany właściciel. Co prawda w ogólności trzeba być gotowym do działania w szerokim zakresie środowisk cyfrowych, zwłaszcza w przypadku uczestnictwa w konkursach, jednak warto się dowiedzieć, jakie są przewidywane środowiska docelowe i jakie rodzaje systemów możesz napotkać. W tej książce będę się skupiał przede wszystkim na systemie Windows oraz wariantach systemu Linux. Przykładowa lista podstawowych kompetencji, jakie powinien mieć Twój zespół, zarówno ataku, jak i obrony, na zawodach CCDC obejmuje znajomość systemów Windows i Unix, doświadczenie z aplikacjami webowymi, sprawność w reagowaniu na incydenty, umiejętność pracy w czerwonym zespole i umiejętność prowadzenia analizy metodami inżynierii wstecznej. Oprócz tego zastosowanie ma też mnóstwo innych umiejętności, na przykład poszukiwanie rodzajów podatności na zagrożenia, monitorowanie sieci, wzmacnianie bezpieczeństwa domen i budowanie infrastruktury — oraz wiele innych. Obszary kompetencji, w których rozwój postanowisz zainwestować, powinny odzwierciedlać przyjętą ogólną strategię działania oraz wpisywać się w realizację pożądanych mocnych stron zespołu. Oznacza to także, że należy inwestować w elementy infrastruktury oraz narzędzia, które wspierają stosowanie wybranych obszarów kompetencji, a także w szkolenia zespołu w tym zakresie.

Plany awaryjne w kontekście kompetencji zespołu powinny dotyczyć powoływania i utrzymywania zespołów zapasowych posiadających wymagane kompetencje oraz tworzenia wszechstronnego programu szkoleniowego, który pozwoli członkom zespołu uzupełnić wiedzę o nowe obszary kompetencyjne. Formułę takiego programu szkoleniowego musisz dobrać do potrzeb i możliwości zespołu — to mogą być cotygodniowe spotkania edukacyjne, mniej formalne pogadanki w porze obiadowej lub zupełnie sformalizowane kwartalne sesje szkoleniowe. Zespół powinien spotykać się regularnie, aby członkowie mieli możliwość podzielenia się *przemyśleniami i wnioskami z dotychczasowych działań* (ang. *lessons learned*). Następnie warto zaplanować indywidualne programy szkoleniowe skupione wokół umiejętności, które członkowie zespołu chcą rozwinąć. Szkolenia formalne są często najlepszą metodą, by szybko wprowadzić członków zespołu w nowe obszary. Warto przyjrzeć się ofercie instytutu SANS, który ma bardzo bogatą ofertę cyberszkoleń w atrakcyjnych cenach, co jest szczególnie istotne, gdy masz napięty budżet[6]. Istnieje także wiele darmowych zasobów cyberszkoleń, ale najważniejsze to zapewnić pracownikom czas na naukę. Jednym z moich ulubionych zbiorów darmowych

szkoleń dotyczących niskopoziomowych umiejętności technicznych jest serwis *https://opensecuritytraining.info/*, zawierający ponad 23 doskonałe kursy i liczne materiały wideo[7]. Kolejnym ciekawym źródłem darmowych szkoleń jest serwis Cybrary i choć oferowane tam kursy nie są tak szczegółowe jak w poprzednim serwisie, to bardzo dobrze sprawdza się stosowany podział na ścieżki kariery, obejmujące wiele adekwatnych umiejętności. Szkolenia Cybrary są zdecydowanie produktami wysokiej jakości[8].

Aby cały zespół odnosił jak najwięcej korzyści z indywidualnych szkoleń, warto przyjąć zasadę, że każdy, kto nabędzie nową umiejętność lub pozna nową technikę, przygotowuje prezentację na jej temat dla pozostałych kolegów. Musisz pamiętać, że nawet doświadczeni gracze będą potrzebowali czasu na poznawanie nowych umiejętności i rozwój posiadanych. I nie zapominaj, że szkolenia są świetne, ale nie zastąpią prawdziwego doświadczenia. Zaraz po szkoleniu członkowie zespołu mogą wnieść dużo do pracy całego zespołu, ale trzeba upewnić się, że ich nowo nabyte umiejętności zostaną wykorzystane szybko i będą wykorzystywane możliwie długo. Jeżeli pozwolą na to czas i harmonogram, to młodsi członkowie zespołu powinni towarzyszyć bardziej doświadczonym w ich zadaniach i uczyć się przez obserwację oraz nadzorowane wykonywanie pracy. W takich wypadkach zwykle proszę nowych członków, aby zweryfikowali aktualność odpowiedniej dokumentacji — w tym celu proszę ich o robienie dodatkowych notatek z pracy wspólnej z doświadczonymi kolegami, aby mogli zaktualizować dokumenty wiki.

Planowanie operacyjne

Planowanie operacyjne ma za zadanie pomóc operatorom w bezpośrednim przygotowaniu do nadchodzącego wydarzenia oraz pomyślnie je przebyć. Plany operacyjne mogą przyjmować postać szczegółowych instrukcji (ang. *runbook*) zawierających podstawowe informacje operacyjne, definicji przepływów pracy (ang. *workflow*) lub opisów zadań technicznych. Plany operacyjne mogą wynikać wprost ze zdefiniowanych wysokopoziomowych celów lub szczególnych warunków określonych dla konkretnej potyczki cyfrowej, na przykład określonych reguł, do których operatorzy muszą się stosować. Ten poziom planowania ułatwia wykonywanie procesów bez zakłóceń oraz pomaga operatorom wznowić działania, jeżeli na czymś utkną. Można przygotowywać plany operacyjne ogólne, stosowane we wszystkich operacjach, lub plany dla konkretnych wydarzeń. W tym drugim przypadku powinny być przygotowywane w oparciu o ogólne cele i szczególne okoliczności, charakterystyczne dla danej operacji. W przypadku rzeczywistych operacji cyberbezpieczeństwa przygotowanie dopasowanych planów wymaga przeznaczenia istotnych nakładów sił i środków na przeprowadzenie rozpoznania, aby prawidłowo ustalić technologie będące celem ataku lub prawidłowo zidentyfikować faktycznie zagrażających aktorów. W ramach konkursów przygotowania takie mogą być prostsze. Często wystarczy sporządzić arkusz kalkulacyjny zawierający listę wszystkich urządzeń pracujących w danym środowisku z zaznaczeniem tych, na których uruchomione zostały kluczowe usługi, a następnie przypisać do każdego z nich wybranego członka zespołu z zadaniem oceny stanu bezpieczeństwa urządzenia lub dokonania włamania. Planowanie operacyjne można także traktować jako zbiór strategii do zastosowania lub procedur dla zespołu. Dzięki stworzeniu zbioru strategii wraz z instrukcjami ich realizacji można zapewnić szczelność stosowanych procesów. Kolejnym logicznym krokiem jest automatyzacja tak zdefiniowanych działań. Na przykład pewna instrukcja operacyjna może nakazywać operatorowi prowadzenie działań z użyciem

maszyny wirtualnej, aby zredukować negatywne skutki przejęcia kontroli nad systemem przez przeciwnika, ograniczyć możliwości rozprowadzania szkodliwego oprogramowania oraz utrudnić identyfikację operatora. Innowacją, jaką mógłby przygotować jeden z członków zespołu, byłoby stworzenie wzorcowego obrazu maszyny wirtualnej, tak zwanej „złotej kopii", oraz przygotowanie automatycznych skryptów do uruchamiania nowych instancji maszyn, gdy tylko członkowie zespołu ich potrzebują. Co więcej, takie maszyny wirtualne mogłyby być od razu wyposażone we wszystkie narzędzia i konfiguracje wykorzystywane przez zespół. Każde z takich automatycznych rozwiązań powinno zostać udokumentowane, a do oryginalnej instrukcji operacyjnej powinny zostać wprowadzone zmiany uwzględniające kroki automatyczne. Jeżeli automatyczne narzędzie będzie się rozrastać, to w pewnym momencie warto rozważyć utworzenie dedykowanego projektu, służącego do długofalowego wsparcia i rozwoju narzędzia, z użyciem prawidłowego cyklu rozwoju oprogramowania.

Dokumenty procedur szczegółowych powinny zawierać wskazówki dotyczące opisywanej techniki lub procesu, aby członek zespołu mógł rozwiać ewentualne wątpliwości powstałe podczas prowadzenia operacji. W treści procedur powinny się znajdować odnośniki do zewnętrznych źródeł informacji opisujących zagadnienie bardziej szczegółowo oraz dostarczających wiedzy kontekstowej, na przykład odpowiedzi na pytanie, dlaczego konkretne narzędzie lub proces może pomóc w realizacji techniki. W procedurach, które przynoszą najwięcej korzyści operatorom, zwykle zamieszczane są także anegdotyczne opisy doświadczeń związanych z daną techniką, odnośniki do opisów przypadków szczególnych i ekstremalnych użycia techniki lub narzędzia oraz odnośniki do wcześniejszych implementacji techniki lub narzędzia, na których autorzy procedury się wzorowali. Warto także zamieszczać w treściach procedur opisy typowych sygnałów ostrzegawczych o błędnym przebiegu wykonania lub oznak wykorzystywania podstępów przez przeciwnika. Z takimi opisami powinny być powiązane plany awaryjne, na przykład zarejestrowanie incydentu bezpieczeństwa, jeżeli istnieje podejrzenie zmanipulowania narzędzi obronnych, lub przełączenie się w tryb reagowania bezpośredniego, jeżeli mogło dojść do błędnego raportowania. Procedury szczegółowe powinny być zwięzłe i atomowe w sensie poruszanej tematyki — w ten sposób będą pozostawały elastyczne i dosyć łatwo będzie można je łączyć w szersze plany operacyjne. Przez opracowanie zawczasu celów operacyjnych oraz procedur szczegółowych możesz przygotować swój zespół do szybkich działań pod dużą presją, jakich należy się spodziewać w cyberkonflikcie, zwłaszcza w ramach rywalizacji konkursowej.

Kolejnym elementem planowania operacyjnego powinno być ustalenie metod pomiaru postępów dokonywanych przez zespół. Wybór odpowiednich **kluczowych wskaźników efektywności** (ang. *key performance indicators*, KPI) pomoże zaobserwować zmiany efektywności pracy na przestrzeni czasu. Najlepiej, gdy pomiary wartości wykorzystywanych do określania wskaźników KPI są zbierane i zachowywane w trybie automatycznym — automatyzacja pozwoli uniknąć ręcznej, mrówczej pracy zbierania wartości pomiarowych potrzebnych do zarządzania zespołem. Jak już wspomniałem, gra w konflikt bezpieczeństwa komputerowego jest asymetryczna, więc omówię oddzielnie przykłady wskaźników dla zespołów ataku i obrony. Nawet w obrębie tych zespołów może istnieć duże zróżnicowanie obserwowanych wskaźników KPI ze względu na znaczne różnice w definicjach ról, których efektywność jest mierzona. W dalszej części rozdziału omówię konkretne przykłady wskaźników właściwych różnym rolom. Warto także przypomnieć, że informatyka jest ze swojej natury niesamowicie skomplikowaną dziedziną, więc czasami wartości mierzone dla analizy wskaźników KPI mogą być zaburzone przez wpływ innych

czynników, przez co obserwowany obraz będzie zafałszowany. Dobrym przykładem takiej sytuacji jest zespół obrony starający się osiągnąć krótkie czasy wykrywania incydentów bezpieczeństwa, badania ich i rozwiązywania, dążąc do osiągnięcia wymarzonych wartości, opisanych przez zasadę 1/10/60[9]. Możliwe, że w wykorzystywanym przez taki zespół chmurowym rozwiązaniu EDR występuje opóźnienie pomiędzy zebraniem a przetworzeniem zawartości dzienników zdarzeń — na przykład do odebrania i przetworzenia powiadomienia w usłudze chmurowej mogą być potrzebne 3 do 5 minut. W efekcie zespół, dopóki będzie korzystać z tej usługi chmurowej, nie będzie nigdy w stanie osiągnąć wykrywania incydentów w ciągu pierwszej minuty od ich wystąpienia, bez względu na to, jak doskonale zostaną skonfigurowane pozostałe elementy infrastruktury obronnej. Dlatego bardzo ważne jest, aby dobrze zrozumieć możliwości i ograniczenia swojego środowiska przy ustalaniu rodzajów mierzonych wartości. Pamiętaj, że ustalenie referencyjnych wartości bazowych dla wskaźników może wymagać wykonania kilku rund pomiarowych.

Podczas przygotowań do uczestnictwa w konflikcie Twój zespół powinien zawczasu opracować plany jego zakończenia. Szczegółowo omówię ten temat w rozdziale 8., „Sprzątanie", ale już na etapie planowania musisz wiedzieć, jak powinna się zakończyć pomyślnie przeprowadzona operacja.

Po stronie obrony zakończenie konfliktu oznacza usunięcie agresora z bronionego środowiska. Obrońcy potrzebują przede wszystkim umiejętności przeprowadzania *analizy przyczyn źródłowych* (ang. *root cause analysis*, RCA) i ustalenia sposobu, w jaki agresor dostał się do bronionej infrastruktury, aby zablokować tę ścieżkę dostępu na przyszłość. Po stronie ataku potrzebna jest umiejętność oceny, kiedy należy opuścić atakowane środowisko, by uniknąć wykrycia. Plany powinny także obejmować sytuacje, gdy operacja rozwinie się w niespodziewany sposób, a może nawet obróci się na korzyść przeciwnika. Zespół ataku powinien zaplanować swoją odpowiedź między innymi na wykrycie kampanii ataku przez obrońców, upublicznienie narzędzi ataku lub nawet ustalenie tożsamości operatorów. Często takie planowanie nazywa się **bezpieczeństwem programu**. Oto jak Matthew Monte opisał je w swojej książce *Network Attacks and Exploitation: A Framework*: „Bezpieczeństwo programu opiera się na zasadzie ograniczania szkód powstałych w wyniku naruszenia bezpieczeństwa operacji. Należy założyć, że pewne operacje zostaną wykryte i zneutralizowane, nawet jeżeli zespół atakujący jest najlepszy w swoim obszarze. (…) Należy dopilnować, żeby fiasko jednej operacji nie zagroziło pozostałym". Bardzo istotne jest, by zespół ataku miał opracowane metody pobierania zdobytych danych i opuszczania atakowanego środowiska po osiągnięciu stawianych celów. W zespole atakującym należy także zastanowić się, po czym poznać, że obrońcy skutecznie zareagowali na incydent — oraz czy w takiej sytuacji należy opuścić infrastrukturę, czy może zaangażować dodatkowe siły i środki, aby ponowić próbę infiltracji. Zespół obrońców powinien rozważać te same tematy, choć z własnej perspektywy — zaniechanie tego może doprowadzić do skutecznego powtórzenia takiego samego ataku.

W dalszej części rozdziału przejdę od planowania do instalacji elementów infrastruktury i narzędzi, których każda ze stron będzie potrzebować dla wsparcia własnych operacji. Po obu stronach konfliktu będzie potrzebne całkiem sporo trwałej infrastruktury. Wykorzystywane narzędzia są szalenie istotnym elementem operacji prowadzonych przez każdy z zespołów, ale ze względu na asymetrię wpisaną w tę grę omówię oddzielnie narzędzia ataku i obrony. Nawet jeżeli zwykle uczestniczysz w zawodach po jednej stronie konfliktu, to bardzo namawiam Cię

do zrozumienia narzędzi oraz infrastruktury przeciwnika. Jak powiedział Sun Zi, „kto zna przeciwnika i zna siebie, nie musi obawiać się wyniku nawet stu bitew". Nie sposób przecenić wagi zrozumienia narzędzi i możliwości przeciwnika, gdyż wyznaczają one opcje, jakie przeciwnik ma dostępne. Moim zdaniem wcieleniem tej zasady jest Dave Cowen, lider czerwonego zespołu w ogólnokrajowej edycji zawodów CCDC. Na co dzień Dave jest dyrektorem odpowiedzialnym za obszar reakcji na incydenty bezpieczeństwa i prowadzi operacje defensywne przeciwko rzeczywistym agresorom. W wolnym czasie przewodzi ochotnikom tworzącym czerwony zespół, dzięki czemu może uczyć się myśleć jak agresor oraz może zdobyć praktyczne doświadczenie w korzystaniu z technik ofensywnych. Jeżeli potrafisz wykorzystać słabości infrastruktury bezpieczeństwa przeciwnika, to możesz zdobyć gigantyczną przewagę w toczonym konflikcie. W kolejnych podrozdziałach pokażę, jak ogromna ilość technologii oraz trwałej infrastruktury jest wykorzystywana po obu stronach konfliktu i że ta infrastruktura bezpieczeństwa też może stać się celem działań strony przeciwnej.

Perspektywa obrony

W tym podrozdziale skupię się na planowaniu, umiejętnościach, narzędziach i infrastrukturze charakterystycznych dla zespołu obrony. Wiele z tych narzędzi może być wykorzystywane samodzielnie do prowadzenia analiz lub w połączeniu z innymi narzędziami, pozwalając osiągnąć bardziej złożone cele. Pokażę, że przygotowanie infrastruktury wspierającej współpracę w zespole przed rozpoczęciem właściwego wydarzenia zaoszczędzi dużo cennego czasu w trakcie prowadzenia operacji. Jak powiedział Lew Tołstoj, „dwaj najpotężniejsi wojownicy to cierpliwość i czas". Rozumiem to tak, że jeżeli mądrze użyjemy dostępnego czasu i cierpliwie będziemy budować systemy obronne, to będziemy znacznie silniejsi w chwili napotkania przeciwnika. Słyszałem porównanie obrony do zestawu sieci budowanych podobnie do sieci pajęczych. Rozwijając to porównanie, sieć musi być wystarczająco duża, aby pokryć całą chronioną przestrzeń, a także na tyle elastyczna, by bezzwłocznie zaalarmować obrońców, gdy coś w nią wpadnie. Co prawda stworzenie sieci zajmuje pająkowi sporo czasu, ale uzyskany rezultat znacząco podnosi skuteczność jego polowań. Raz utworzona sieć wymaga angażowania wysiłku, kompetencji i zasobów, by utrzymać ją na właściwym poziomie sprawności. Aby tym bardziej podkreślić, że przygotowania są kluczowe do obrony, warto zaznaczyć, że agresor potrzebuje tylko jednego udanego włamania, aby uzyskać punkt zaczepienia w sieci. Skuteczna obrona za to powinna udaremniać 100% ataków kierowanych przeciw bronionej infrastrukturze. Jest to niemal niemożliwe, więc należy przygotować procesy reagowania na incydenty umożliwiające identyfikację zagrożenia, ograniczenie jego negatywnych skutków i likwidację, gdy już dojdzie do nieuniknionego udanego włamania. Możesz na przykład stworzyć sieć maszyn działających jako bufor przed właściwymi ochranianymi maszynami i umożliwiających wykrycie i identyfikację włamań. Jest to realizacja koncepcji *obrony w głąb*, wspomnianej w poprzednim rozdziale. Jeżeli jest praktycznie niemożliwe, by zapobiec włamaniu do pojedynczego systemu, to należy stworzyć sieć dobrze zabezpieczonych systemów, przez które atakujący będzie musiał się przedostać w drodze do swojego celu — taki łańcuch włamań na kolejne systemy można wykryć i zareagować na niego. Jeżeli zaangażujesz do realizacji strategii wiele różnych technologii defensywnych, to znacząco zwiększasz prawdopodobieństwo wykrycia postępującego ataku. Podczas planowania ważne jest, żeby potraktować priorytetowo przygotowanie infrastruktury potrzebnej

do realizacji strategii dopasowanej do potrzeb Twojego zespołu. Należy także zaplanować opcje postępowania na wypadek utraty dostępu do krytycznej infrastruktury, co może się zawsze wydarzyć podczas konfliktu. To jest szalenie istotna część wspomnianego wcześniej planowania awaryjnego — w żargonie korporacyjnym byłaby to część strategicznego planowania dla zachowania ciągłości działania. Zgodnie z najlepszymi branżowymi praktykami postępowania należy wykorzystywać alternatywne metody i narzędzia nie tylko jako infrastrukturę zapasową, ale także do aktywnej weryfikacji działania podstawowych narzędzi i metod, aby mieć pewność, że nie zostały oszukane przez atakujących. Bardzo często agresorzy instalują nieautoryzowane metody dostępu do systemu lub stosując różne podstępy starają się zmienić rezultaty działania narzędzi monitorujących, aby zmylić obrońców.

Powszechnie się uznaje, że pierwszą inwestycją, którą powinien poczynić zespół obrony, jest stworzenie rozwiązania do tworzenia dzienników zdarzeń bezpieczeństwa, agregacji pochodzących z nich danych i powiadamiania o wykrytych anomaliach. W tym celu niezbędne jest generowanie wpisów do dzienników ze wszystkich krytycznych systemów oraz przechowywanie ich w centralnym zbiorze. W przypadku istotnych incydentów zawartość dzienników bezpieczeństwa może być wykorzystywana do analizy sytuacji, w tym do rekonstrukcji wydarzeń dla celów dowodowych. Do zbierania danych bezpieczeństwa z aktywnych elementów infrastruktury zwykle używane są specjalne programy lub agenty. Obszar zbierania danych o bezpieczeństwie cyfrowym przeważnie dzielę na trzy kategorie: telemetrię sieciową, telemetrię urządzeń oraz telemetrię aplikacji — tę ostatnią kategorię nazywam też telemetrią opartą na dziennikach zdarzeń. W dalszej części książki będę omawiał wszystkie trzy rodzaje, ponieważ każdy z nich ma swoje mocne i słabe strony. Pokażę, jak wykorzystywać agenty programowe do łączenia danych pochodzących z tych kategorii w jeden centralny zbiór używany przez analityków bezpieczeństwa do prowadzenia analiz oceniających. Na przykład monitorowanie sieci może pomóc w identyfikowaniu nieznanych urządzeń podłączonych do bronionej sieci, podczas gdy analiza dzienników zdarzeń z poziomu aplikacji może ujawnić szczegóły wykorzystania protokołu komunikacyjnego wskazującego na szkodliwe użycie aplikacji. W trakcie konkursów staram się na pierwszym miejscu postawić widoczność zdarzeń i urządzeń w sieci komputerowej, następnie skupić się na analizie urządzeń, a dopiero na sam koniec analizować poziom aplikacji — w ten sposób łatwiej jest wykryć nową próbę włamania. Uruchomione na urządzeniach agenty zbierające dane są nieocenioną pomocą podczas badania pojedynczych włamań, gdyż dostarczają szczegółowych informacji na temat infekcji komputera szkodliwym oprogramowaniem oraz możliwych sposobów reakcji. Pomiary bezpieczeństwa na poziomie aplikacji są zwykle najistotniejsze podczas incydentów w obrębie organizacji biznesowych. Przeważnie są one powiązane z istotą prowadzonej działalności i mogą wskazać obecność agresora dążącego do osiągnięcia swoich celów lub nadużywającego Twoich danych. Często agresorzy wykorzystują *zasadę człowieczeństwa*, ukrywając atak pod pozorem działań prawdziwego użytkownika — obserwacje na poziomie aplikacji mogą umożliwić wykrycie takich działań. Przykładowo jeżeli głównym produktem Twojej organizacji jest masowa wieloosobowa gra sieciowa, to zbieranie informacji o zdarzeniach i wskaźnikach bezpieczeństwa w obrębie samego kodu gry najpewniej szybciej wykaże istnienie nadużyć niż poszukiwanie śladów włamania do serwerów wewnętrznych. Niemniej dane aplikacji są mniej użytecznie w kontekście zawodów bezpieczeństwa, gdyż w nich zazwyczaj kładzie się nacisk przede wszystkim na penetrację sieci, a używane aplikacje sieciowe są przeważnie dosyć proste. Zacznę od zagadnienia tworzenia danych dla dzienników zdarzeń bezpieczeństwa z różnych źródeł, opisując kwestie telemetrii urządzeń, sieci i aplikacji. Następnie przedstawię pokrótce

technologie stosowane do łączenia, sortowania i przeszukiwania zawartości dzienników. Ale przetwarzanie danych z dzienników na tym się nie kończy — po zidentyfikowaniu niepokojących zdarzeń należy dokonać dalszego przetwarzania danych i wzbogacić je o dodatkowe informacje. W tym celu przedstawię metody pobierania, przechowywania i analizy różnorodnych artefaktów. Tytuły kolejnych podrozdziałów możesz potraktować jako skróconą listę projektów, których przeprowadzenie warto rozważyć w ramach planowania prac zespołu obrony, a które pozwolą wytworzyć odpowiednie narzędzia. W każdym z tych obszarów istnieje szereg technik i narzędzi, które można zastosować. Będę się skupiał przede wszystkim na rozwiązaniach darmowych i otwartoźródłowych.

Zbieranie danych

Zacznę od rozwiązań przeznaczonych do monitorowania zdarzeń bezpieczeństwa dotyczących konkretnego komputera. Tradycyjnie używane były w tym celu programy antywirusowe, takie jak McAfee, Microsoft Defender, Symantec Endpoint Protection (SEP), Kaspersky lub ClamAV. Obecnie często uważa się je za przestarzałe, ale wciąż mogą wykryć znane szkodliwe oprogramowanie lub zastosowanie znanych technik ataku. Niektóre pakiety, między innymi SEP lub Kaspersky, mogą także wykrywać anomalie statystyczne, jakie powstają na przykład w przypadku prób ukrywania szkodliwych programów za pomocą różnych technik zaciemniania lub szyfrowania. Programy antywirusowe mogą być bardzo przydatne w środowisku firmowym, chroniąc stacje robocze przed typowymi zagrożeniami, ale ich skuteczność w środowiskach konkursowych jest znacznie mniejsza, ponieważ agresorzy zwykle wykorzystują autorskie oprogramowanie ofensywne. Kolejną klasą rozwiązań są pakiety do *monitorowania działania urządzeń końcowych* (ang. *Endpoint Detection and Response*, EDR), które stanowią współczesne rozwinięcie tradycyjnych skanerów antywirusowych. Platformy EDR, z punktu widzenia operatorów bezpieczeństwa, oferują pewną znaczącą przewagę nad skanerami antywirusowymi: umożliwiają operatorom dowolne przeszukiwanie zgromadzonych danych. Agenty EDR pozwalają także przeprowadzić aktywną reakcję na incydenty, dopóki urządzenie jest online, na przykład poprzez zdalne wykonanie pewnych czynności naprawczych — funkcjonalność ta nazywana jest *live response*. Możliwości aktywnego reagowania są szczególnie przydatne w zmaganiach z żywym agresorem, gdyż pozwalają pokrzyżować jego plany w obrębie konkretnej maszyny. Kolejną zaletą narzędzi EDR jest duża ziarnistość rejestrowania aktywności na monitorowanym komputerze. Na przykład systemy Windows lub OS X w standardowej konfiguracji nie będą zapisywać informacji o utworzonych procesach, atrybutów komend wykonywanych w wierszu poleceń, informacji o załadowanych modułach ani wielu innych. Agenty EDR mogą zostać skonfigurowane, aby zbierać szczegółowe dane pomiarowe o uruchamianych procesach i przesyłać je do centralnego serwera do dalszej analizy lub rekonstrukcji przebiegu incydentu. Odtworzenie przebiegu incydentu jest niezbędne, aby zapobiec podobnym wydarzeniom w przyszłości. Jest to również podstawa do przeprowadzenia *analizy przyczyn źródłowych*. Jak pokażę w rozdziale 8., „Sprzątanie", jeżeli nie przeprowadzisz poprawnej analizy przyczyn zdarzenia, to ryzykujesz, że usunięcie problemu będzie tylko częściowe, przez co atakujący może uzyskać przewagę. Wykorzystując możliwości agenta EDR, można dosyć łatwo przeanalizować przebieg zdarzenia w obrębie jednego urządzenia, a potem wyszukiwać oznaki zastosowania danej techniki ataku lub szkodliwego oprogramowania w pozostałych zarządzanych komputerach, korzystając z agentów na nich zainstalowanych. Dzięki temu możesz poddać weryfikacji stawiane hipotezy bezpieczeństwa

i w konsekwencji usprawnić system powiadamiania o niepokojących zdarzeniach. Omówię dokładniej techniki *poszukiwania luk i przypadków podatności na zagrożenia* w rozdziale 7., „Przez badania do przewagi", pokazując metody identyfikowania nowych rodzajów alertów, nowych artefaktów dowodowych, a nawet nowych źródeł informacji dla dziennika zdarzeń. Rozwiązania EDR umożliwiają zbieranie obszernych informacji o działaniu procesów, w tym listy otwartych plików, aktywnych połączeń sieciowych oraz identyfikatorów używanych obiektów systemowych. Pozwala to skutecznie wykrywać wiele rodzajów szkodliwego oprogramowania, gdyż zamiast skupiać się na atrybutach łatwych do zmiany, na przykład na nazwie pliku, mechanizmy detekcji mogą obserwować istotę działania szkodliwych programów, na przykład liczbę otwieranych plików lub informacje o nawiązywanych połączeń sieciowych. Monitoring behawioralny umożliwia wykrywanie użycia abstrakcyjnych technik, takich jak skanowanie portów lub szyfrowanie plików dla okupu, bez względu na to, w jakim narzędziu zostały zaimplementowane. Kolejną techniką wykrywania włamań w środowiskach firmowych jest zastosowanie narzędzi EDR do *wykrywania anomalii*. W skrócie polega ona na uporządkowaniu wszystkich zebranych danych według pewnego klucza i dokładniejszej analizie przypadków odbiegających od typowych wartości. Często dokładna analiza programów, które występują najrzadziej w środowisku firmowym, pozwala znaleźć niebezpieczne narzędzia. W tym segmencie rynku istnieją liczne rozwiązania komercyjne, na przykład Advanced Threat Protection firmy Microsoft, CrowdStrike, CarbonBlack lub Tanium. Pewnym problemem, przynajmniej z turniejowego punktu widzenia, jest typowa domyślna konfiguracja narzędzi komercyjnych, minimalizująca liczbę fałszywych alarmów. W przypadku infrastruktury bezpieczeństwa budowanej z myślą o operacjach długookresowych ma to sens, ponieważ pozwala zminimalizować zmęczenie analityków wynikające z obsługi wielu zbędnych powiadomień. Jednakże w przypadku konkursów bezpieczeństwa, które charakteryzują się znacznie krótszymi ramami czasowymi i pewnością, że istnieje aktywnie działający agresor, lepiej jest uzyskiwać jak najwięcej jak najdokładniejszych informacji monitorowania na temat bronionych komputerów. Przy odpowiednio bogatym materiale analitycznym możesz starać się wykrywać także mniej spotykane techniki hakerskie lub analizować działanie zaobserwowanych niestandardowych procesów. Osobiście zwykle wybieram rozwiązania EDR typu open source, na przykład OSQuery[10] do wzbogacania zebranej informacji lub GRR Rapid Response[11] do wykonywania dodatkowych weryfikacji podczas prowadzonego śledztwa. Innymi popularnymi narzędziami EDR ze świata open source są Wazuh[12] i Velociraptor[13]. Obie platformy funkcjonują już od dłuższego czasu w świecie cyberbezpieczeństwa i były rozwijane przez lata, dzięki czemu pracują stabilnie i mają bogaty zestaw dostępnych opcji. Rozwiązania służące do zbierania i analizowania danych o zdarzeniach systemowych w obrębie konkretnej maszyny są wspaniałymi narzędziami do szczegółowej analizy przebiegu incydentów bezpieczeństwa w ramach monitorowanego komputera lub do poszukiwania oznak włamania pośród wielu bronionych maszyn.

Monitorowanie sieci może być źródłem niezmiernie istotnych informacji na temat bezpieczeństwa. Przez strategiczne rozmieszczenie punktów analizy ruchu sieciowego możesz zidentyfikować urządzenia, które regularnie komunikują się poprzez sieć, i ustalić, z jakich protokołów korzystają. Na podstawie zebranych danych możesz wykrywać anomalie w ruchu sieciowym lub ewidentnie wrogą komunikację — na przykład porządkując informacje według rodzajów użytych protokołów lub według punktów docelowych. Skuteczne narzędzie do monitorowania sieci pozwala administratorom na stopniowe wzmacnianie jej bezpieczeństwa, ponieważ pomaga zrozumieć, jakie są charakterystyki typowego ruchu sieciowego. Gdy rozpoznasz poprawną

komunikację, to resztę możesz zablokować za pomocą zapór sieciowych. W środowisku konkursowym możesz od ręki zastosować prostą regułę, dopuszczającą wyłącznie komunikację przy użyciu protokołów punktowanych — tym samym znacznie zmniejszasz objętość danych do przebadania przez zespół obrony. Kolejnym krokiem, wynikającym ze stosowania *zasady fizycznego dostępu*, jest objęcie kontrolą wewnętrznego ruchu sieciowego. Służą do tego systemy zapobiegania włamaniom (ang. *Intrusion Prevention System*, IPS), takie jak Suricata, albo wewnętrzne zapory sieciowe. Odpowiednio konfigurując te narzędzia, możesz objąć kwarantanną zainfekowaną maszynę, czyli zupełnie odciąć ją od sieci albo przenieść do wydzielonej wirtualnej sieci VLAN. Izolując wybraną maszynę, powstrzymujesz ruch agresora w obrębie własnej sieci. Twój zespół może zachować dostęp do izolowanej maszyny, dzięki czemu możesz kontynuować analizę i ocenę sytuacji — wystarczy odpowiednio skonfigurować zaporę. Narzędzia monitorowania sieci umożliwiają także analizę sygnałową, dzięki której zespół obrony może obserwować anomalie ruchu sieciowego, nawet jeżeli zespół atakujący będzie starał się ukryć swoją komunikację, na przykład poprzez tunelowanie w innych protokołach lub przy użyciu węzłów pośredniczących. Do obserwacji ruchu sieciowego w ramach przykładów prezentowanych w książce będę używał narzędzi Snort, Suricata, Wireshark i Zeek. Snort dobrze nadaje się do identyfikowania znanych wzorców szkodliwego ruchu sieciowego — będę go używał do skanowania ruchu, podobnie jak stosowane są tradycyjne programy antywirusowe[14]. Suricata także jest narzędziem ułatwiającym identyfikację szkodliwych wzorców w komunikacji sieciowej[15]. Zeek przede wszystkim umożliwia szczegółową analizę treści przekazywanych poprzez najróżniejsze protokoły sieciowe i rejestrowanie szczegółowych informacji o przepływach komunikacji[16]. To są przykłady podstawowych aplikacji monitorujących. Powinny one być na stałe zainstalowane w wybranych miejscach sieci, a gdy zaczną już działać, to będą dostarczać bardzo istotnych informacji. Narzędzia monitorowania sieci bardzo ułatwiają wykrywanie problemów sieciowych i przyspieszają usuwanie usterek. Jeżeli w trakcie zawodów punktowana usługa przestanie działać, to dzięki informacjom z monitoringu sieci możesz szybko ustalić, czy problem wynika z usterki w kierowaniu ruchem sieciowym, czy z nieprawidłowego działania komputera realizującego usługę. Próby wykrywania włamań poprzez analizę dzienników zdarzeń z komputerów można porównać do szukania igły w stogu siana, a monitorowanie sieci — do obserwacji ruchu pojazdów na autostradzie. W tym drugim przypadku nawet przy dużych prędkościach często łatwiej jest zaobserwować nieprawidłowe zachowania i ustalić ich źródło. Sieci i środowiska konkursowe zazwyczaj nie są wyposażone w zapory i urządzenia do monitorowania sieci, ale niemal zawsze można przeorganizować architekturę lub sposób kierowania ruchem tak, aby korzystać z funkcjonalności monitorowania. Zgodnie z *zasadą fizycznego dostępu*, jeżeli kontrolujesz fizyczny dostęp do przełączników sieciowych, to możesz skopiować ruch sieciowy, wykorzystując funkcję analizatora ruchu sieciowego (ang. *Switch Port Analyzer*, SPAN)[17]. Funkcja kopiowania ruchu sieciowego do celów analizy jest też znana pod nazwą *port mirroring*. Inną metodą jest przekierowanie całego ruchu przez jeden z komputerów, aby przekształcić go w urządzenie do monitorowania sieci. Do rejestrowania komunikacji sieciowej służy polecenie `tcpdump`[18], a podany poniżej przykład jego wywołania spowoduje przechwytywanie całego ruchu przesyłanego przez wskazany interfejs, w tym wypadku `eth0`:

```
$ sudo tcpdump -i eth0 -tttt -s 0 -w outfile.pcap
```

Musisz się oczywiście upewnić, czy wybrana maszyna ma łącza sieciowe o wystarczającej przepustowości i odpowiednio duży dysk. Objętość nieprzetworzonych danych o przechwyconych pakietach (`pcap`) przyrasta bardzo szybko, więc będziesz potrzebować znacznej przestrzeni do

ich przechowywania. Należy też na bieżąco obserwować, czy objętość zebranych informacji nie staje się zbyt duża. Wspaniałym narzędziem do przeprowadzania analiz ruchu sieciowego na żywo jest Wireshark[19]. Jest to bardzo popularne narzędzie, wyposażone w graficzny interfejs użytkownika pozwalający operatorom między innymi oznaczać kolorami różne protokoły komunikacyjne oraz aktywnie śledzić wybrane strumienie protokołu TCP. Wireshark zawiera także modularną platformę programistyczną, która umożliwia dodawanie komponentów do interpretacji niestandardowych protokołów — na przykład własnych protokołów przeciwnika rozpracowanych z użyciem metod inżynierii wstecznej[20]. Narzędzia tcdump i Wireshark możesz uruchomić bardzo szybko, ale lepiej jest zainwestować trochę wysiłku i stworzyć rozwiązanie monitorowania sieci nastawione na dłuższe użytkowanie. W tym celu możesz użyć narzędzia tshark, dostarczanego wraz z pakietem Wireshark i uruchamianego z wiersza poleceń. Pozwala ono analizować zawartość przechwyconych pakietów oraz zbierać informacje o zdarzeniach sieciowych. Dzięki temu nie musisz przechowywać ogromnych ilości nieobrobionych danych, za to możesz tworzyć dzienniki zdarzeń o wybranym formacie. Na przykład poniższe polecenie stworzy listy wszystkich źródłowych i docelowych adresów IP, wraz z docelowymi numerami portów, które pojawiały się w przychodzącym i wychodzącym ruchu sieciowym danej maszyny[21]:

```
$ sudo tshark -i eth0 -nn -e ip.src -e ip.dst -e tcp.dstport -Tfields
↪-E separator=, -Y ip > outfile.txt
```

Kolejnym ważnym źródłem informacji o zdarzeniach mogą być rozszerzenia bezpieczeństwa wprowadzane do konkretnych aplikacji. Kwestie bezpieczeństwa często nie są dogłębnie przemyślane na początkowym etapie tworzenia usługi, więc zabezpieczenia są dodawane później, do działającego produktu, zwykle w postaci modułów pośredniczących w komunikacji sieciowej z usługą. Przykładami takich rozwiązań są narzędzia do zabezpieczania poczty elektronicznej (ang. *email security gateway*) lub zapora sieciowa przeznaczona do ochrony aplikacji webowych (ang. *web application firewall*), która kontroluje ruch kierowany do istotnej aplikacji. Narzędzia te również generują wpisy do dzienników zdarzeń oraz alerty, które są kluczowe dla całego obszaru bezpieczeństwa. W wielu organizacjach dominującym wektorem ataku jest phishing, więc sensowne jest wykorzystanie produktów do weryfikacji przychodzącej poczty elektronicznej pod kątem informacji bezpieczeństwa i alarmowania o potencjalnych e-mailach phishingowych — przykładowymi rozwiązaniami są Proofpoint i Agari. Narzędzia tej kategorii pozwalają często wykonać pewne działania w reakcji na pojawiające się zagrożenie — na przykład w przypadku ochrony poczty narzędzia zabezpieczające mogą dawać użytkownikom możliwość zgłaszania podejrzanych wiadomości, a operatorom zabezpieczającym sieć umożliwiać masowe usuwanie szkodliwych e-maili. Wdrożenie takich narzędzi przeważnie wiąże się ze znaczącym kosztem i wymaga specjalistycznych kompetencji, więc jeżeli Twoja organizacja zdecyduje się na ich uruchomienie, to ważne jest, by miały odpowiedni priorytet finansowania i przydziału pracowników. Rozwiązania mogą być zwykle kupowane w modelu licencyjnym lub subskrypcyjnym, a ich dostawcy często oferują wsparcie techniczne. Gdy narzędzia takie zostaną zakupione lub udostępnione w ramach konkursu, należy potraktować ich konfigurację priorytetowo i w pełni wykorzystać dostępne wsparcie techniczne. Inną metodę monitorowania, blisko spokrewnioną z koncepcją aplikacyjnych dzienników zdarzeń, stanowią wskaźniki nadużyć kluczowych usług biznesowych. Jeżeli Twoja organizacja oferuje dostęp do dużych aplikacji webowych, na przykład wspierających handel elektroniczny lub hosting maszyn wirtualnych, to zdecydowanie powinieneś zbierać szczegółowe informacje na temat używania i nadużywania usług. Przykładowymi wskaźnikami mogą być liczba transakcji wykonywanych z pojedynczego

konta i lista użytkowników najsilniej obciążających API aplikacji. Zebrane informacje można przetwarzać za pomocą metod analizy behawioralnej lub wykrywania anomalii, podobnie jak przy wcześniej omawianych informacjach rejestrowanych w dziennikach zdarzeń. Analiza behawioralna może polegać na obserwacji szybkości, z jaką użytkownicy przemieszczają się pomiędzy ekranami aplikacji — możesz w ten sposób wykryć próby nadużyć z wykorzystaniem automatyzacji. Przykładem poszukiwania anomalii jest uporządkowanie informacji o zdarzeniach logowania według źródłowych adresów IP i dokładniejsze zbadanie często powtarzających się podobnych wartości, co pozwala zaobserwować potencjalne próby masowego przejmowania kont użytkowników. Kolejnym ważnym źródłem danych analitycznych są wewnętrzne narzędzia i aplikacje Twojego zespołu. Ich analiza pod kątem nadużyć lub nietypowych logowań może wskazać, że konto któregoś z członków zostało przejęte lub że doszło do zdrady i zagrożeniem jest osoba z wewnątrz organizacji. Analiza informacji z wewnętrznych narzędzi raczej nie będzie zadaniem priorytetowym podczas prowadzenia działań w reakcji na istniejące naruszenie bezpieczeństwa, ale kompletne jej pominięcie może pogrzebać całą operację zapewniania bezpieczeństwa.

Dzięki elementom infrastruktury służącym do aktywnej obrony możemy nakłonić agresorów do ujawnienia ich obecności w sieci. Narzędzia te widoczne są jako elementy infrastruktury podatne na włamania, aby skłonić atakujących do próby przejęcia[22]. Infrastruktura aktywnej obrony będzie często wspominana na kartach tej książki, gdyż daje wielką przewagę obronie poprzez możliwość zastawiania pułapek na agresorów. Pokażę, jak zasada *ukazywania fałszu* pomaga w wykrywaniu atakujących. Przykładami aktywnej obrony są serwery pułapki (ang. *honeypot*), sztuczne rekordy danych (ang. *honey token*) i fałszywe elementy infrastruktury. Pozornie te elementy infrastruktury wydają się bez znaczenia, ale mądrze stosując *zasadę podstępu*, omawianą w poprzednim rozdziale, możesz stworzyć fałszywe, łatwe do zinfiltrowania, ale wiarygodnie wyglądające cele dla agresorów. Gdy hakerzy spróbują uzyskać dostęp do pułapki, to jednocześnie ujawnią swoją obecność, a zespół obrony zyska znaczącą przewagę. Koszt wdrożenia takich rozwiązań jest swego rodzaju zakładem hazardowym o skuteczność podstępu. Osobiście uważam, że ta taktyka powinna być stosowana jedynie pomocniczo do metod zbierania informacji opisanych powyżej. Samodzielne jej użycie raczej nie przyniesie oszałamiających rezultatów. Aby pułapki działały naprawdę skutecznie, muszą istnieć łatwe ścieżki dostępu do nich. Haker próbujący włamać się na typowe konto użytkownika powinien w naturalny sposób odkryć taką ścieżkę i złapać się w pułapkę. Repozytorium Awsome Honeypots na GitHubie zawiera całe mnóstwo przykładów pułapek (*https://github.com/paralax/awesome-honeypots*), ale najważniejsze to wybrać takie, które pasują do Twojej sieci. Liczba przykładów w tym zbiorze i w internecie jest ogromna, więc masz duże szanse znalezienia pułapki, której będziesz mógł użyć. Pamiętaj, aby umieszczać pułapki rozsądnie, gdyż zbyt ukryta lub zbyt ewidentna pułapka może pozostać nieaktywowana przez lata. Niemniej jeżeli wystawisz ponętny, łatwy do zauważenia i wiarygodnie wyglądający cel, to będzie on doskonałym wskaźnikiem obecności agresora w sieci.

Zarządzanie danymi

Wprowadzenie metod agregacji informacji o zdarzeniach z różnych dzienników może się przyczynić do największych oszczędności czasu zespołu obrony. Moim zdaniem przetwarzanie potokowe dzienników zdarzeń jest jednym z niedocenianych cudów współczesnej infrastruktury

obronnej. Po prostu w przeważającej liczbie publikacji dotyczących obrony ten temat nie jest traktowany z należytą uwagą. W większości korporacyjnych infrastruktur IT zbieranie informacji o zdarzeniach już jest wszechobecne i działa w tle większości środowisk produkcyjnych. Jeżeli Twoja organizacja może podłączyć się do tych istniejących przepływów informacji, to możesz oszczędzić mnóstwo wysiłku na zarządzanie infrastrukturą. W środowisku konkursowym jest mało prawdopodobne, aby podobna infrastruktura była dostępna, więc aby uzyskać możliwości scentralizowanego przetwarzania logów, najpewniej będziesz musiał połączyć wiele prostych narzędzi. Informacje o zdarzeniach możesz zbierać w centralnej lokalizacji w bardzo prosty sposób, na przykład przesyłając wszystkie dane na jeden serwer, albo w bardzo skomplikowany, na przykład instalując *system zarządzania informacjami i zdarzeniami bezpieczeństwa* (ang. *security information and event management*, SIEM). Często elementy rejestrujące zdarzenia w dziennikach mogą być wbudowane w aplikację SIEM, ale nie zawsze tak jest — separacja rozwiązań może być korzystna dla funkcjonalności rejestrowania zdarzeń. Usługi Filebeat[23] lub Logstash mogą być używane dodatkowo, oprócz bardziej rozbudowanych rozwiązań, takich jak Splunk. Z kolei narzędzie Splunk może być wykorzystane do wzbogacania i normalizowania wpisów w dziennikach zdarzeń, zanim zostaną przesłane do systemu SIEM. Użycie potoków przetwarzania dzienników zdarzeń oznacza, że możesz edytować i standaryzować informacje w miarę ich pozyskiwania — niezależnie od tego, czy rozwiązanie klasy SIEM jest stosowane do ostatecznej analizy, czy nie. Nawet jeżeli nie używasz scentralizowanego rozwiązania do przetwarzania dzienników zdarzeń SIEM, to wciąż możesz wzbogacać pozyskaną informację o zdarzeniach za pomocą potoków przetwarzania lub przesyłać ją do jednej lokalizacji. W najprostszym przypadku wykorzystywanie scentralizowanego zarządzania dziennikami zdarzeń może polegać na użyciu domyślnych możliwości narzędzi rsyslog, SMB czy nawet dziennika zdarzeń systemu Windows[24]. Prosta agregacja logów różni się od użycia rozwiązania SIEM — w tym drugim przypadku rozwiązanie SIEM udostępnia możliwości indeksowania i przeszukiwania danych, powiadamiania o alertach, a nawet pozwala na graficzną prezentację zebranych informacji. Dzięki możliwościom błyskawicznego zbierania i porządkowania danych dowodowych możesz dosyć szybko określić zakres i zasięg incydentu. Niezależnie od technicznych szczegółów implementacji, jeżeli będziesz mógł uruchomić i przeprowadzić analizę całego środowiska, pracując na jednym komputerze, to spodziewane oszczędności czasu będą gigantyczne.

W pełni wykorzystywany system SIEM może znacząco pomóc w porządkowaniu i przeszukiwaniu dzienników zdarzeń. Produkty takie jak Splunk lub Elasticsearch oferują bogate możliwości przeszukiwania i łączenia wielu zbiorów danych. Wykorzystanie takich narzędzi w trakcie konkursów zwykle pozostaje w sferze marzeń, chyba że organizatorzy zapewniają do nich dostęp albo przynajmniej infrastrukturę, na której można takie narzędzie uruchomić. Niemniej w każdym przypadku organizowania obrony rzeczywistych systemów narzędzia SIEM są bardzo istotne. Możliwości indeksowania wielu źródeł informacji o zdarzeniach, łącznego ich przeszukiwania, przekształcania danych na bieżąco, łączenia z zewnętrznymi źródłami danych i prezentacji zawartości w formie tabel lub wykresów są bezcenne przy prowadzeniu wszelkich analiz. Usługi oferowane przez wspomniany już Splunk dominują nad innymi w swoim obszarze, ze względu na możliwości produktu w zakresie indeksowania i przekształcania danych. Pakiet Splunk zawiera wiele zaawansowanych funkcjonalności, na przykład moduł analizy zachowania użytkowników (ang. *User Behavior Analytics*, UBA), udostępniający wyszukiwanie korelacji pomiędzy zawartością dzienników zdarzeń w celu wykrywania świadczących o włamaniu anomalii w działaniach użytkowników[25]. Pakiet zawiera także platformę integracyjną,

za pomocą której operatorzy mogą tworzyć własne komponenty i uzyskiwać dostęp do własnych usług lub prezentować dane w unikatowy sposób. Komercyjny produkt Splunk ma swój odpowiednik w świecie open source — HELK[26], który oferuje za darmo podobne możliwości. Pakiet HELK jest połączeniem wielu technologii open source służących do rejestrowania i przetwarzania informacji o zdarzeniach, między innymi ELK, czyli Elasticsearch, Logstash i Kibana. Jest to wspaniały przykład zastosowania *zasady innowacji* do wytworzenia rozwiązań dla obszaru bezpieczeństwa. W ramach tej książki będę korzystał głównie z narzędzia Elasticsearch i pakietu HELK, ponieważ są one darmowe i łatwo dostępne[27]. Jeżeli zależy Ci na ograniczaniu liczby narzędzi instalowanych w Twojej infrastrukturze, to w ELK jest także standardowo dostępna funkcjonalność powiadamiania i generowania alertów. Istnieją również rozwiązania SIEM przeznaczone do indeksowania i analizy dzienników zdarzeń dotyczących sieci. Na przykład program Vast może odczytywać zarówno logi generowane przez pakiet Zeek, jak i nieprzetworzone zapisy pakietów sieciowych `pcap`, umożliwiając przeszukiwanie tych zbiorów danych[28]. Podstawową informacją, jaką będziemy pobierać z całej sieci i nad którą będziemy pracować, będzie zawartość dzienników zdarzeń. Rozwiązania klasy SIEM pomagają ujednolicić tę zawartość poprzez odwzorowanie ich na wspólny format danych, dzięki czemu możesz skutecznie przeszukiwać wszystkie dostępne informacje, a nie tylko pojedyncze zbiory.

Miłym dodatkiem byłoby posiadanie *rozwiązania do organizowania, automatyzacji i realizacji odpowiedzi bezpieczeństwa* (ang. *Security Orchestration, Automation and Response*, SOAR). W przypadku dużych organizacji aplikacje klasy SOAR stanowią tkankę łączącą niezliczone narzędzia bezpieczeństwa w rozwiązanie SIEM. Taka aplikacja sięga do wielu lokalizacji w sieci i zestawia zawartość alertów z innymi informacjami, pozwalającymi lepiej zrozumieć kontekst powiadomienia. Narzędzie takie może wzbogacić treść powiadomienia o dodatkowe informacje, na przykład uzupełnić informacje o użytkowniku o wartości jego atrybutów pobranych z usługi katalogowej Active Directory. Solidnym przykładem platformy klasy SOAR w świecie open source jest aplikacja Cortex[29]. Wdrożenie bardziej rozbudowanych aplikacji, łączących wiele elementów infrastruktury, jest zwykle sporą inwestycją, ale możliwości oceny incydentów otrzymywane przez operatorów centrum bezpieczeństwa (*Security Operations Center*, SOC), są nie do przecenienia. Rozwiązanie takie umożliwia operatorom scentralizowane przeprowadzanie weryfikacji i innych działań na wszystkich elementach infrastruktury. Analitycy nie tylko otrzymują więcej informacji kontekstowej wraz z każdym alertem, ale dzięki automatycznym akcjom mogą szybciej oceniać wagę incydentów. Gdy zaczyna się robić gorąco, to możliwość wizualizacji na jednym ekranie pełnego kontekstu zarejestrowanych zdarzeń jest niezbędna do przeprowadzenia szybkiej oceny incydentu. Konieczność przełączania się między wieloma narzędziami, technologiami lub interfejsami użytkownika zajmuje dużo czasu i przyczynia się do popełniania błędów. Rozwiązania klasy SOAR pomagają zespołowi obrony rozwiązać ten problem w szybki i powtarzalny sposób.

Bardzo ważnym elementem rozwiązania SIEM lub SOAR jest zbiór definicji zdarzeń i alertów — koniecznie uwzględnij w planowaniu regularne weryfikacje i aktualizacje jego zawartości. Najlepiej, gdy zarządzanie tym zbiorem odbywa się poza aplikacją SIEM lub SOAR, dzięki czemu zespół może niezależnie weryfikować i poprawiać jego zawartość. Należy stworzyć odpowiednie elementy infrastruktury w tym celu — na przykład możesz użyć rozwiązania Threat Alert Logic Repository (TALR)[30], które jest repozytorium reguł detekcji zdarzeń i alertów podzielonych na kategorie według powiązanych funkcjonalności, taktyk i działania. Dzięki zastosowaniu

tego lub podobnego rozwiązania znacząco wzrośnie zdolność detekcji zagrożeń w Twoim środowisku, gdyż będziesz mógł od razu posługiwać się wieloma sprawdzonymi regułami. W 2013 roku firma Mandiant opracowała platformę OpenIOC, udostępniając do publicznego użytkowania standardowy format opisu zdarzeń i alertów[31]. Nazwa narzędzia pochodzi od określenia *indicators of compromise* (IOC), czyli oznaki przeprowadzonej infiltracji systemu. Wspominam o narzędzi OpenIOC, ponieważ definiowany w nim format zawiera kluczową moim zdaniem cechę definicji alertu: logikę kombinatoryczną. Główną wadą tradycyjnych rozwiązań antywirusowych było zbytnie uproszczenie logiki detekcji — z powodu braku możliwości łączenia wielu źródeł danych lub nieuwzględnienia informacji kontekstowej narzędzia te nie były w stanie wykryć bardziej zaawansowanych technik ataku. Platforma OpenIOC udostępnia obrońcom rozbudowaną logikę definiowania alertów, której działanie może się opierać na różnorodnym materiale dowodowym. Bardzo ważne jest, by w działaniach zespołu obrony ustandaryzować zapis logiki detekcji oraz upewnić się, że nie zawiera ona luk, niezależnie od konkretnie wybranych formatu i składni opisu zdarzeń. Usprawni to weryfikację istniejących definicji oraz ustalanie strategii dla przyszłych działań detekcyjnych. Kolejnym rodzajem elementów, które Twój zespół powinien zbierać, katalogować i regularnie weryfikować, są szczegółowe procedury wykonania działań (ang. *playbook*). Stosowanie tych procedur pozwala jeszcze bardziej rozszerzyć funkcjonalności detekcji i powiadamiania poprzez ustalenie automatycznych akcji, które powinny zostać wykonane, gdy system SOAR wykryje nieprawidłową sytuację i zgłosi alert[32]. Logika wykrywania niepoprawnych sytuacji i powiadamiania o nich powinna być w centrum uwagi zespołu obrony, ponieważ stanowi to trzon działań, do których są szkoleni operatorzy. Informacje te koniecznie muszą być spisane i skodyfikowane, a nie przekazywane wyłącznie jako tradycja ustna członków zespołu — ułatwi to szerzenie wiedzy w zespole oraz regularną weryfikację, czy wykorzystywane definicje wciąż są poprawne i użyteczne. Co więcej, zorganizowanie stosowanej logiki wykrywania i powiadamiania w postaci sformalizowanych struktur pozwala dostrzec luki i słabe punkty w procesie detekcji. Jeżeli w Twojej organizacji istnieje zespół operacji ofensywnych, to dobrym pomysłem jest przeprowadzenie z nim symulacji wrogich działań i weryfikacja istniejących procedur detekcji i powiadamiania. Doskonałą metodą przygotowania do cyberkonfliktów, zarówno konkursowych, jak i rzeczywistych, jest zapoznawanie się z powszechnie stosowanymi technikami oraz uzupełnianie braków w zdefiniowanej logice detekcji. Dla zespołu prowadzącego operacje obronne rzeczywiste, a nie w ramach konkursów, ważnym narzędziem są systemy zarządzania incydentami, odpowiedziami na nie i zgłoszonymi alertami. W środowiskach firmowych służą one do zapewnienia w dłuższym okresie czasu ciągłości śledzenia obsługiwanych przypadków przez kolejne zmiany operatorów. Pomagają one także dopilnować, by wszystkie zgłoszenia zostały obsłużone. Z kolei w trakcie zawodów do tego celu może wystarczyć prosta lista podejrzanych maszyn, z której będą one wykreślane po zakończeniu weryfikacji. Niezależnie od wybranego sposobu organizacji pracy kluczowe jest zapewnienie systemowego wsparcia do szybkiej weryfikacji powiadomień, grupowania pojedynczych powiadomień w bardziej złożone incydenty, przesyłania zgłoszeń do obsługi w innych zespołach oraz ustalania, nad którymi przypadkami (i konkretnymi krokami w tych przypadkach) operatorzy aktywnie pracują. W prostych przypadkach może wystarczyć arkusz kalkulacyjny do śledzenia listy zainfekowanych komputerów lub działań naprawczych. Informację o tym, kto aktualnie zajmuje się którym artefaktem dowodowym, możesz przechowywać w zakładkach, z których każda odpowiada konkretnemu urządzeniu. Do obsługi bardziej skomplikowanych sytuacji skuteczniejsze może być zastosowanie przeznaczonego do tego systemu, w którym użytkownicy mogą przechowywać i oznaczać dodatkowe materiały dowodowe związane z danym przypadkiem.

W ramach pakietu HELK dostępne jest narzędzie ElastAlert[33]. Jest ono także dostępne w ramach systemu do zarządzania alertami TheHive. ElastAlert można dosyć łatwo zainstalować i zintegrować z innymi systemami. Pozwala ono wysyłać powiadomienia e-mail do operatorów o wykrytych przypadkach, a weryfikacja alertu może być przeprowadzona w ramach systemu TheHive[34]. Narzędzie TheHive pozwala także na integrację obsługi alertów z innymi używanymi w Twojej organizacji usługami, między innymi z usługą Cortex, która umożliwia wykonywanie działań bezpośrednio na podstawie zawartości powiadomień. Połączenie narzędzi TheHive i Cortex zapewni operatorom dostęp do bardzo potężnego rozwiązania z wykorzystaniem pojedynczego interfejsu użytkownika — w innym wypadku operatorzy mogą być zmuszeni do ciągłego przeskakiwania między oddzielnymi systemami podczas obsługi powiadomienia lub przeciwdziałania incydentowi.

Kolejnymi przydatnymi, choć nie niezbędnymi aplikacjami mogą być narzędzia wymiany i zbierania informacji. Takie rozwiązania jak MISP mogą pobierać informacje z wielu źródeł i łączyć je w jednej lokalizacji w celu analizy i śledzenia[35]. Inną aplikacją tej klasy jest Collaborative Research Into Threats (CRITS) — umożliwia ona łączenie informacji z wielu źródeł i śledzenie powiązań pomiędzy artefaktami w wewnętrznej bazie danych[36]. Możesz także wykupić dostęp do profesjonalnych serwisów świadczących usługi zbierania danych, jednakże zwykle wiąże się to z uiszczeniem sporej opłaty rocznej. Platformy przetwarzania informacji zainstalowane w obrębie własnej infrastruktury mogą być zintegrowane z rozwiązaniami SIEM lub SOAR, dzięki czemu istnieje możliwość wzbogacania treści alertów o dodatkowe dane, pobrane z narzędzi wymiany informacji. Odpowiednio zintegrowane aplikacje mogą automatycznie uruchamiać platformy oceny zagrożeń dla zebranych artefaktów dowodowych, przenosić artefakty do magazynów informacji dowodowych, a nawet rozpoczynać procedurę reakcji na incydent bezpieczeństwa. Oprócz bardzo użytecznej funkcjonalności dołączania do analizy zewnętrznych informacji o zagrożeniach aplikacje tego typu zwykle umożliwiając dodawanie szczegółowych notatek i komentarzy odnośnie do zebranych danych o zagrożeniach. Bardzo ważne jest wiedzieć, że inny członek zespołu badał już wcześniej dane zagrożenie lub spotkał się z podobnymi oznakami przy innej okazji. Kolejnym nabytkiem wartym rozważenia przez zespół obrony jest prywatny system zarządzania materiałami dowodowymi. Jest to naturalne rozwinięcie systemu do zarządzania incydentami bezpieczeństwa — system, który umożliwia przechowywanie i katalogowanie zebranych artefaktów dowodowych. Zbiór takich informacji ułatwia przeprowadzenie analizy pozdarzeniowej, ustalenie sprawstwa ataku lub po prostu uzyskanie przewagi nad przeciwnikiem. Narzędzia wymiany informacji i zarządzania materiałem dowodowym mogą wydawać się zbędne, dopóki nie uruchomisz reszty wymaganych narzędzi, ale nawet proste rozwiązanie przyniesie wymierne długofalowe korzyści, ułatwiając prowadzenie analiz szkodliwego oprogramowania. W idealnej sytuacji rozwiązanie tej klasy powinno być zintegrowane z systemem zarządzania zgłoszeniami, ale często wystarczą nawet dzielony dysk sieciowy lub serwer SFTP, na których można wykonywać kopie zapasowe zebranych artefaktów. Warto zmodyfikować uprawnienia dostępowe tak, aby użytkownicy nie mogli modyfikować ani usuwać materiałów stworzonych przez innych. Dobrym pomysłem jest skonfigurowanie uprawnień repozytorium tak, aby pliki nie mogły być zmieniane po utworzeniu — w ten sposób artefakty i materiały dowodowe będą zabezpieczone przed przypadkowym nadpisaniem oraz przed próbami manipulacji. Jest to prosty sposób na zapewnienie *integralności* artefaktów oraz uszczelnienie *autoryzacji* dostępu w aplikacji. W systemie Linux efekt taki można uzyskać przez ustawienie atrybutu *sticky bit* dla katalogu repozytorium artefaktów. Wartość tego atrybutu umożliwia

dodatkową kontrolę uprawnień dostępu do plików — gdy ma on wartość niezerową, to tylko właściciel lub administrator mogą usuwać lub modyfikować pliki w katalogu. Ustawienie atrybutu *sticky bit* dla katalogu następuje poprzez wykonanie polecenia `chmod +t nazwa_katalogu`. Można pójść o krok dalej i sprawić, by plik stał się niezmienny, tak że nawet właściciel nie będzie mógł go zmodyfikować ani usunąć — w tym celu należy wykonać polecenie `chattr +i nazwa_pliku.txt`. Aby móc jeszcze ściślej kontrolować integralność wgrywanych plików, możesz wdrożyć rozwiązanie, które będzie wyliczać ich kryptograficzną funkcję skrótu (ang. *hash*). Główne informacje warte przechowywania to sama zawartość pliku, wartość jej funkcji skrótu, data utworzenia i, być może, identyfikator zapisującego ją użytkownika. Poniżej zamieszczam przykład krótkiego skryptu, który pokazuje, jak proste może być wprowadzanie innowacyjnych rozwiązań realizujących omawiane koncepcje. Ten konkretny skrypt, napisany w języku Python 3.6, służy do obserwacji zawartości katalogu. W przypadku pojawienia się nowego pliku zmieniane są atrybuty zbioru, aby był niezmienny, a w dzienniku zdarzeń zapisywana jest data utworzenia pliku, jego pełna ścieżka dostępowa oraz wartość funkcji skrótu. Program może być uruchomiony wyłącznie pod kontrolą systemu Linux, ponieważ używane jest w nim polecenie `chattr`. Zachowaj ostrożność, by nie podać katalogu, z którego skrypt został uruchomiony, jako katalogu monitorowanego — w takim wypadku skrypt wpadnie w pętlę nieskończoną, gdyż będą wciąż wykrywane zmiany pliku dziennika zdarzeń aktualizowanego w wyniku wykrycia modyfikacji pliku.

```
import sys
import time
import logging
import hashlib
import subprocess
# Komentarz 1: Importowanie istotnych elementów biblioteki Watchdog służącej do obserwacji plików
# lub folderów
from watchdog.observers import Observer
from watchdog.events import LoggingEventHandler
# Komentarz 2: Konfiguracja wyjściowego pliku dziennika zdarzeń
logging.basicConfig(filename="file_integrity.txt",
                    filemode='a',
                    level=logging.INFO,
                    format='%(asctime)s - %(message)s',
                    datefmt='%Y-%m-%d %H:%M:%S')
hasher = hashlib.sha1()

def main():
  path = input("Podaj ścieżkę do monitorowanego katalogu: ")
  # Komentarz 3: Uruchomienie metody obsługi zdarzeń oraz metody obserwatora katalogu docelowego
  event_handler = LoggingEventHandler()
  event_handler.on_created = on_created
  observer = Observer()
  observer.schedule(event_handler, path, recursive=True)
  observer.start()
  try:
    while True:
      time.sleep(1)
  except KeyboardInterrupt:
    observer.stop()
  observer.join()
```

```
def on_created(event):
  # Komentarz 4: Akcje do wykonania, gdy nowy plik zostanie zapisany
  subprocess.Popen(['chattr', '+i', event.src_path], bufsize=1)
  with open(event.src_path, 'rb') as afile:
    buf = afile.read()
    hasher.update(buf)
  logging.info("Artefakt: %s \nSkrót SHA1: %s\n", event.src_path,
  ↪hasher.hexdigest())
  print("Utworzono nowy plik: {}\n Skrót SHA1: {}\n".format(event.src_path,
  ↪hasher.hexdigest()))

if __name__ == "__main__":
  main()
```

Powyższy skrypt ma dosyć prostą konstrukcję, ale jest niesamowicie przydatny. Możesz użyć tego programu do uruchomienia niemal każdego działania w wyniku zaobserwowanych zmian stanu pliku. Możesz go łączyć w łańcuchy przetwarzania z innymi narzędziami, dzięki czemu możesz uruchomić niemal każdy rodzaj analizy i niemal dowolne zadanie. Przyjrzyjmy się nieco dokładniej zawartości tego skryptu. Poniżej linii zawierającej *Komentarz 1* wykonywany jest import elementów z biblioteki `watchdog`. Biblioteka `watchdog` jest niezbędna do wykrywania zdarzeń i reagowania na nie. Możliwe, że operatorzy będą musieli pobrać bibliotekę `watchdog` na swoje maszyny za pomocą menedżera pakietów Python-Pip. Następnie, poniżej linii zawierającej *Komentarz 2*, ustawiana jest konfiguracja składowych biblioteki `watchdog`, w wyniku której będzie możliwe zapisywanie w pliku tekstowym dziennika. Konfiguracja zawiera nazwę pliku wyjściowego, tryb dostępu do pliku (otwierany w trybie dopisywania) oraz format komunikatów. Poniżej linii zawierającej *Komentarz 3* zarejestrowana zostaje metoda obsługi zdarzeń. Jako metoda obsługi zdarzenia utworzenia pliku `event_handler.on_created` zostaje zarejestrowana funkcja `on_created`. Następnie powoływana jest instancja obserwatora, a obserwator zostaje powiązany z wcześniej zarejestrowaną metodą obsługi zdarzeń i z docelową ścieżką do monitorowanego katalogu. Po tym następuje wystartowanie obserwatora. We fragmencie listingu poniżej linii zawierającej *Komentarz 4* zostały zapisane akcje wybrane do uruchomienia, gdy obserwator wykryje zapis do nowego pliku. W podanym przykładzie uruchamiany jest podproces, aby wykonać polecenie systemowe `chattr +i` na świeżo zapisanym pliku. W kolejnych krokach metody znajdującej się pod linią zawierającą *Komentarz 4* nowo utworzony plik zostaje otworzony do odczytu, wyliczany jest jego skrót `SHA1`, a następnie do pliku dziennika zostaje zapisana nazwa pliku i wartość jego skrótu. W kolejnym podrozdziale zajmę się dokładniej możliwościami analiz, jakie można przeprowadzić na zbieranych plikach.

Narzędzia analityczne

Kolejnym zestawem narzędzi, które uważam za absolutnie niezbędne, są narzędzia do przeprowadzania analiz i oceny zagrożenia w obrębie komputera, na którym zostały uruchomione. Dzięki nim możesz uzyskać dodatkowe informacje o zagrożeniach, na przykład zbadać podejrzane procesy lub przeanalizować artefakty odnalezione w systemie. Narzędzia analityczne są niezbędne operatorom, aby mogli lepiej zrozumieć działanie bronionych systemów operacyjnych i zawartość odnalezionych artefaktów czy aby zidentyfikować nierozpoznane dane. Dobrymi przykładami lokalnie działających narzędzi analitycznych dla systemu Windows są Autoruns, Process

Monitor lub Process Explorer z pakietu SysInternals Suite[37]. Umożliwiają one analitykom przyjrzenie się zainstalowanym na komputerze lub uruchomionym programom i wątkom, a także prześledzenie wywołań systemowych wykonywanych przez te programy. Narzędzia analityczne mogą także umożliwiać badanie różnorodnego materiału dowodowego poprzez pobieranie plików, dzienników zdarzeń i artefaktów lub prowadzenie analizy składniowej. Na przykład rozwiązania takie jak Yara umożliwiają szybkie przeszukiwanie dysku lub katalogu pod kątem interesujących artefaktów zawartych w plikach[38]. Kolejne narzędzia, takie jak Binwalk[39] i Scalpel[40], umożliwiają ekstrakcję osadzonej zawartości plików na podstawie wyników poszukiwania przez program Yara. Dzięki łączeniu lokalnych narzędzi analitycznych w łańcuchy wykonania możesz szybko stworzyć procedury do wyszukiwania plików z ukrytą zawartością („koni trojańskich") lub konkretnych osadzonych artefaktów[41]. Tradycyjne narzędzia informatyki śledczej, takie jak The Sleuth Kit i RedLine, także pozwalają uzyskiwać niesamowite rezultaty, choć konkretne wyniki mogą zależeć od rodzaju badanego systemu[42]. Pakiet The Sleuth Kit wyśmienicie nadaje się do przeprowadzania analiz obrazów dysków oraz artefaktów znajdujących się w tych obrazach[43]. Z kolei narzędzi takich jak RedLine i Volatility można użyć do analizy pamięci w locie[44]. Dzięki temu możliwe jest przeprowadzenie szybkiej oceny zagrożeń dla maszyny oraz pobranie artefaktów z pamięci ulotnej do przeprowadzenia analizy. W zespołach obrony, które prowadzę, staram się przygotowywać standardowy zestaw narzędzi, których członkowie zespołu mogą używać w trakcie typowych zadań analitycznych. Oprócz samych narzędzi przygotowujemy też szczegółowe procedury ich wykorzystania. Dzięki takiemu postępowaniu możemy osiągnąć standaryzację narzędzi analitycznych w obrębie zespołu, a także zapewniać, że członkowie stopniowo stają się ekspertami.

Niesamowitym przykładem zastosowania *zasady innowacji* jest narzędzie BLUESPAWN[45], opracowane przez reprezentację Uniwersytetu Wirginii na zawodach CCDC. Rozwiązanie przypomina scyzoryk szwajcarski i składa się z narzędzi, które studenci wcześniej automatyzowali na potrzeby swojego uczestnictwa w turnieju. Pakiet BLUESPAWN został napisany w języku C++ i może analizować wyłącznie system Windows, ale jest prawdziwym kombajnem, jeżeli chodzi o oferowaną funkcjonalność. Drużyna uniwersytecka twierdzi, że BLUESPAWN zwielokrotnia możliwości zespołu, a członkowie bardziej obeznani z systemem Linux mogą w łatwy sposób dokonywać oceny bezpieczeństwa systemu Windows. BLUESPAWN łączy wiele funkcjonalności, udostępniając je w następujących trybach pracy: *monitorowanie*, *poszukiwanie*, *skanowanie*, *ograniczanie* i *reagowanie*. Program generuje gigantyczną ilość informacji, które, w połączeniu z różnorodnymi procedurami szczegółowymi, pozwalają operatorom zespołu obrony analizować i interpretować sytuację, a także na nią reagować. BLUESPAWN pozwala zautomatyzować wiele operacji związanych z aktualizowaniem i uszczelnianiem systemu oraz z wykrywaniem w czasie rzeczywistym wykorzystania konkretnych technik ataku. W efekcie operatorzy dostają do ręki narzędzie umożliwiające łatwe i powtarzalne wykonywanie typowych działań. Wykorzystanie pakietu znacząco poprawia skuteczność zespołu, zwłaszcza że do efektywnego użycia narzędzia potrzebne jest jedynie krótkie szkolenie i stworzenie pewnej liczby typowych procedur szczegółowych[46]. W rozdziale 3., „Najlepiej być niewidzialnym (działania w pamięci)", zaprezentuję, jak autorzy BLUESPAWN wykorzystali je do automatyzacji użycia narzędzia PE-Sieve lub wykrywania sesji powłoki narzędzia Cobalt Strike[47], oraz przedstawię dokładniej metody wykrywania takich zagrożeń. Zastosowanie innowacyjnych technik zdecydowanie wytrąca z rytmu zespół ofensywny i daje obrońcom ogromną przewagę, zwiększając ich możliwości oceny zagrożeń i reagowania na nie.

Platformy oceny szkodliwego oprogramowania, zarówno statyczne, jak i dynamiczne, mogą być bardzo cennym narzędziem w rękach zespołu analitycznego. Takie systemy mogą stanowić tani zamiennik pracy faktycznego specjalisty od inżynierii wstecznej, a ich użycie może zaoszczędzić czas analitykom lub inżynierom. Przykładem statycznej platformy analitycznej jest Viper, dostarczany jako produkt open source. Użytkownicy mogą dołączać do narzędzia własne rozszerzenia, utworzone w języku Python, dzięki którym mogą implementować dowolne operacje wykonywane na pojedynczych artefaktach dowodowych. Taka platforma może łączyć funkcjonalności repozytorium danych dowodowych i narzędzia analitycznego[48]. Przykładowe rozszerzenia mogą zweryfikować, czy badany plik jest wykonywalny, następnie wyszukać w nim potrzebne dane, takie jak adresy URL lub IP, i wydobyć je, a potem uruchomić proces wzbogacania w oparciu o dane z aplikacji zarządzania informacjami o zagrożeniach. Narzędzie Viper można łatwo zintegrować z platformą analizy dynamicznej, na przykład Cuckoo Sandbox, i w ten sposób udostępnić analitykom szczegółowe informacje o próbie uruchomienia analizowanego pliku binarnego[49]. Analiza dynamiczna jest bardzo efektywnym sposobem uzyskania dodatkowych informacji o szkodliwym oprogramowaniu i polega na próbie uruchomienie badanego pliku w ściśle monitorowanym wydzielonym środowisku (tzw. „piaskownicy", od ang. *sandbox*). Obserwacja działającego programu często może dostarczyć informacji niemożliwych do uzyskania poprzez analizę statyczną. Czasem skonfigurowanie i uruchomienie dynamicznego środowiska dla takiej analizy, szczególnie rozwiązania Cuckoo Sandbox, może nastręczać wyjątkowych trudności z powodu różnych problemów kompatybilności pomiędzy wspieranymi rodzajami i wersjami hipernadzorców, agentów i maszyn wirtualnych. Jeżeli interesuje Cię wykorzystanie narzędzia Cuckoo, to warto zapoznać się z projektem BoomBox w serwisie GitHub. Rozwiązanie stworzone w ramach tego projektu ma za zadanie przeprowadzić pełną instalację i konfigurację platformy Cuckoo, skrywając całą złożoność za fasadą kilku prostych poleceń[50]. Często w infrastrukturze wspierającej analizy dynamiczne instalowany jest komponent INetSim, służący do symulowania ruchu sieciowego. Obecność ruchu sieciowego w zamkniętym środowisku analitycznym może sprawić, że szkodliwe oprogramowanie aktywuje i ujawni więcej swoich cech[51]. W ramach turniejów raczej nie będzie udostępniona infrastruktura prywatna pozwalająca uruchomić platformy analizy dynamicznej lub statycznej — ale mogą być udostępnione analogiczne usługi chmurowe. Serwisy takie jak VirusTotal[52], Joe Sandbox[53], Anyrun[54] i HybridAnalysis[55] mogą znacznie poprawić zdolność zespołu do przeprowadzenia analizy przechwyconego szkodliwego oprogramowania, ale ich wadą jest konieczność wykorzystania usługi publicznej. W obrębie niektórych usług publicznych, na przykład VirusTotal, hakerzy mogą konstruować reguły Yara i za ich pomocą poszukiwać własnych autorskich komponentów pośród wgranych na platformę przykładów szkodliwego oprogramowania. Odnalezienie takich przykładów może oznaczać utratę przewagi przez obrońców, ponieważ agresorzy mają potwierdzenie przechwycenia próbek ich ofensywnego oprogramowania.

W operacjach obronnych bardzo przydatne są także narzędzia do przekształcania danych, takie jak CyberChef[56]. Należy je traktować jako aplikacje pomocnicze, ponieważ przy ich użyciu raczej nie da się zrealizować głównych celów procesu detekcji. Niemniej zespół obrony może skrócić czas przetwarzania danych oraz poprawić bezpieczeństwo operacyjne poprzez zastosowanie bezpiecznej centralnej usługi, która umożliwia wykonywanie typowych przekształceń danych. W tym obszarze także można twórczo wykorzystać *zasadę innowacji* — na przykład poprzez powiązanie w jedną usługę webową kilku omawianych wcześniej narzędzi analitycznych uruchamianych lokalnie na maszynie lub stworzenie nowego narzędzia wykorzystującego takie

usługi. Świetnym przykładem zastosowania innowacji jest aplikacja webowa Pure Funky Magic (PFM)[57]. Zawiera ona wiele użytecznych narzędzi analitycznych, a dzięki centralnemu dostępowi wszyscy analitycy w zespole mogą korzystać z tych samych reguł transformacyjnych. Natomiast do współdzielenia pomiędzy członkami zespołu informacji o zagrożeniach i zebranych danych świetnie nadają się rozwiązania do tworzenia notatek w postaci map myśli, takie jak Maltego[58]. Dzięki takim narzędziom możesz zwielokrotnić skuteczność wymiany informacji o zagrożeniach w obrębie zespołu i podnieść jego zdolności operacyjne.

Rozważ wykorzystanie przez zespół niebieski elementów działań ofensywnych. Przede wszystkim chodzi o zarządzanie rodzajami podatności na zagrożenia i kompetencje w wykonywaniu testów penetracyjnych, w szczególności umiejętność skanowania własnej infrastruktury w poszukiwaniu przypadków podatności na zagrożenia. Wiele na ten temat dowiesz się z kolejnych podrozdziałów, opisujących perspektywę ataku, choć myślę, że taktyki utrzymywania stałego nieautoryzowanego dostępu i oszukiwania obrońców nie będą miały zastosowania, skoro Twój zespół będzie samodzielnie oceniał podatność bronionych środowisk na ataki. W trakcie zawodów bezpieczeństwa Pros V Joes zespoły składają się z nie więcej niż 10 osób — zwykle jedna lub dwie z nich zajmują się działaniami ofensywnymi. W tym konkursie architektury sieci wszystkich zespołów są identyczne, więc zespoły rozpoczynają pracę od poszukiwania przypadków podatności w ramach własnej sieci. Takie podejście ma szereg zalet: bliskość elementów infrastruktury w sieci powoduje, że wyniki skanowania są uzyskiwane szybciej i z większą precyzją, zespół może opracować i przetestować odpowiednie narzędzia ofensywne przy zachowaniu bezpieczeństwa operacyjnego, a na koniec można pozbawić przeciwnika punktów, włamując się do jego infrastruktury. Najpierw zespół skupia się na zabezpieczeniu własnych systemów w rozsądnym stopniu, a następnie przygotowuje automatyzacje, by uruchamiać skanowanie w regularnych odstępach, i nakierowuje przygotowane wcześniej narzędzia ofensywne na infrastrukturę przeciwnika.

Jak widać istnieje wiele elementów infrastruktury, które powinny być zainstalowane i uruchomione przed wystąpieniem incydentu bezpieczeństwa albo przynajmniej przygotowane do szybkiego wdrożenia bezpośrednio po wystąpieniu incydentu. Potrzeba nie lada umiejętności i intensywnego planowania, aby wybrać właściwą kolejność i harmonogram wdrażania potrzebnych technologii, nie zakłócając jednocześnie prowadzenia podstawowych działań operacyjnych. Jeżeli chcesz w praktyce wypróbować niektóre z omawianych technologii, to bardzo polecam zapoznanie się z platformą Security Onion 2[59]. Jest to rozwinięcie popularnego narzędzia Security Onion wzbogacone o wiele z narzędzi opisywanych w tym rozdziale.

Security Onion 2 można zainstalować na oddzielnych maszynach lub razem z innymi aplikacjami w środowisku produkcyjnym. Natomiast wiele z opisanych przeze mnie elementów infrastruktury będzie wymagać wykorzystania dedykowanego sprzętu, często w ramach klastra współbieżnie działających maszyn. Security Onion 2 możesz używać na przykład do sprawdzania potencjalnych rozwiązań, w szczególności czy integracja z pozostałymi usługami odbywa się bez przeszkód. Możesz też korzystać z tego pakietu do przeprowadzania oceny zagrożeń w lokalnym środowisku i wytwarzania własnych narzędzi czy nawet zainstalować go na niewielkim środowisku produkcyjnym. Niemniej należy rozważać, czy wdrożenie wydzielonych rozwiązań nie będzie lepiej spełniało Twoich potrzeb. Zawsze trzeba zacząć od kilku niezbędnych kroków, takich jak zrozumienie środowiska, w którym zespół będzie operować, pozyskanie

odpowiednich kompetencji do zespołu czy opracowanie planu rozwoju — ale potem wdrożenie i uruchomienie każdego z elementów infrastruktury będzie przedsięwzięciem samym w sobie. Ważne, aby nie uruchamiać większej liczby projektów, niż zespół będzie w stanie przeprowadzić, więc wybór pierwszych wdrażanych elementów jest kluczowy. Dużo zależy od obsady, jaka jest dostępna, ale moim zdaniem najważniejsze są komponenty do zbierania danych telemetrycznych na temat bezpieczeństwa, następnie rozwiązania do agregacji zawartości dzienników zdarzeń i prowadzenia analiz artefaktów czy wreszcie narzędzia umożliwiające operatorom reagowanie na bieżąco i prowadzenie przeciwdziałań bezpośrednio na zagrożonych urządzeniach.

Kluczowe wskaźniki efektywności zespołu obrony

Bardzo przydatne jest ustalenie wskaźników umożliwiających pomiar efektywności zespołu[60]. W tym celu powstały kluczowe wskaźniki efektywności (ang. *Key Performance Indicators*, KPI), czyli dobrze określone wskaźniki pomiarowe, które pozwalają porównywać, jak skuteczność zespołu wypada na tle innych podobnych zespołów, oraz mierzyć, jak skuteczność zmienia się w czasie. Typowymi wskaźnikami pomiarowymi dla zespołu obrony mogą być średni czas potrzebny do wykrycia ataku, średni czas reakcji na incydent i średni czas rozwiązania incydentu (zgodnie ze wspomnianą wcześniej zasadą 1/10/60). Wśród innych stosowanych wskaźników warto wymienić liczbę zbadanych incydentów, średni czas potrzebny do zbadania incydentu, najdłuższy czas badania incydentu czy liczbę zweryfikowanych reguł. Dzięki pomiarom tych wartości zespół będzie mógł zidentyfikować luki i słabe punkty sposobu działania zespołu — mogą to być aktywności kończące się niepowodzeniem bez wyraźnej informacji o błędzie lub obszary, w których potrzebne jest zwiększenie liczby przydzielonych zasobów. Często o dziedzinie bezpieczeństwa myśli się zero-jedynkowo — albo pełen sukces, albo pełna porażka. W rzeczywistości liczba możliwych rezultatów jest niezliczona i zawsze można znaleźć obszary do usprawnienia[61]. Pamiętaj, że jedną z korzyści planowania długofalowego jest stopniowa poprawa działania, a wskaźniki są narzędziem pozwalającym potwierdzić, czy rozwój zespołu zmierza we właściwym kierunku.

Perspektywa ataku

Omówię teraz umiejętności, narzędzia i elementy infrastruktury, jakie zespół ataku może pozyskać przed rozpoczęciem operacji. John Lambert napisał na Twitterze: „Jeżeli uważasz, że badacze technik ofensywnych powinni się wstydzić, to najwyraźniej nie rozumiesz skutków ich prac. Atak i obrona nie są sobie równe. Obrona jest dzieckiem ataku”[62]. Wprawdzie uważam, że nazywanie obrony „dzieckiem ataku” jest sporym wyolbrzymieniem, ale dużo prawdy jest w stwierdzeniu, że zespoły obrony bardzo wiele uczą się na podstawie wyników badań nad metodami ataku. W domenie cyberbezpieczeństwa systemy obronne zazwyczaj zmieniają się dosyć powoli, statycznie i w reakcji na działania atakujących, do których należy wykonanie pierwszego ruchu. Jak pokażę w dalszej części tej książki, to zazwyczaj atakujący wykonują pierwszy ruch lub przejmują inicjatywę po zakończeniu początkowych prac organizacyjnych. Działania ofensywne mają, w porównaniu do defensywy, znacznie bardziej ulotny charakter. Ogólnie strona ataku zajmuje się znacznie mniejszą liczbą elementów infrastruktury, ponieważ większość jej

wysiłku skupia się na infrastrukturze celu ataku, a także na pozostawianiu jak najmniejszej ilości śladów. Ponieważ strona atakująca zarządza znacznie mniej rozległą infrastrukturą i ma bardziej ulotną naturę, znacznie łatwiej może zmieniać stosowane rozwiązania lub automatyzować zadania za pomocą prostych skryptów. Stosowanie metod automatycznej instalacji oraz redukowanie czasu potrzebnego na instalację będzie kluczowe dla strony atakującej, w miarę jak zagłębia się w proces ataku i na bieżąco dostosowuje swoje taktyki. Jeżeli potrafisz przejmować kolejne maszyny szybciej, niż obrona nadąża z ich weryfikacją, i możesz zmieniać swoje narzędzia ofensywne w trakcie ataku, to obrońcy będą mogli tylko zgadywać, na jakie elementy ich infrastruktury rozszerza się włamanie. Podobnie jak w przypadku narzędzi dla obrony, bardzo ważne jest, aby opracować narzędzia alternatywne i infrastrukturę zapasową, na wypadek gdyby Twój zespół musiał całkowicie zmienić sposób działania.

Skanowanie i wykorzystywanie przypadków podatności na zagrożenia

Narzędzia do skanowania i enumeracji są oczami i rękami zespołu ataku. Pozwalają zbadać atakowaną infrastrukturę i poznać stosowane w niej technologie. Atakujący rozpoczynają swoją działalność operacyjną od skanowania, więc powinni mieć te techniki dobrze opanowane. Podobnie jak dobra partia szachów rozpoczyna się jednym z kilku pożądanych ruchów, tak atakujący ma kilka pożądanych sposobów na przeprowadzenie początkowego skanowania, aby zrozumieć atakowane środowisko. Wybrana technologia skanowania powinna być dobrze rozumiana przez członków zespołu i możliwie mocno zautomatyzowana, aby operatorzy dysponowali skryptami bardziej ogólnymi, skrywającymi złożoność uruchamiania konkretnych narzędzi skanujących. Atakujący będą potrzebowali między innymi narzędzi do skanowania sieci, narzędzi do analizy przypadków podatności na zagrożenia, narzędzi enumerujących zawartość domen oraz narzędzi do skanowania aplikacji webowych. Narzędziami do skanowania sieci są na przykład Nmap i masscan. Działają one poprzez rozsyłanie pakietów protokołów TCP/IP w celu identyfikacji aktywnych maszyn i usług w sieci. Dzięki automatyzacji przeprowadzania takich skanów można łatwo uruchamiać je co pewien czas, a z analizy różnic uzyskanych w kolejnych przebiegach stworzyć dynamiczny obraz otwieranych i blokowanych portów w badanym systemie. W zespole czerwonym National CCDC wykorzystujemy rozwiązanie Docker, które uruchamia skanowanie za pomocą ulotnych instancji maszyn wirtualnych zmieniających adresy IP przed każdą rundą skanowania, a po zakończonym cyklu przesyła operatorom skonsolidowane raporty. Bardzo przydatne jest porównywanie wyników skanowania pochodzących z różnych punktów w czasie, gdyż pozwala zaobserwować zmiany w sieci, jakie w tym okresie zaszły. AutoRecon jest wspaniałym przykładem produktu open source, który pokazuje, jak innowacyjne wykorzystanie istniejących technologii może dawać przewagę nad przeciwnikiem[63]. Kolejnym interesującym nabytkiem może być Scantron, który oferuje skanowanie z wykorzystaniem rozproszonych agentów i udostępnia wygodny interfejs użytkownika[64]. Strona ofensywna ma też do dyspozycji narzędzia enumeracyjne, które będą sprawdzać, czy w pracującym w atakowanym środowisku oprogramowaniu istnieją znane przypadki podatności na zagrożenia. Przykładami takich skanerów podatności są narzędzia nmap-vulners[65], OpenVas[66] i Metasploit[67]. Umożliwiają one odszukanie pośród wcześniej zidentyfikowanego oprogramowania konkretnych przypadków podatnych na ataki.

Nmap-vulners pozwala atakującym połączyć operację skanowania portów bezpośrednio z enumeracją przypadków podatności. Podobnie zespół ataku może wyniki skanowania uzyskane przez Nmap przekazać bezpośrednio do pakietu Metasploit, w którym nastąpi próba uzyskania nieautoryzowanego dostępu. W zespole czerwonym National CCDC bardzo intensywnie wykorzystujemy skrypty RC pakietu Metasploit do automatyzacji i łączenia w łańcuchy wykonania narzędzi wykorzystujących pewne rodzaje podatności, by uzyskać nieautoryzowany dostęp, narzędzi uruchamiających sesje zwrotne powłoki, a nawet narzędzi do przekazywania złośliwego oprogramowania na atakowane maszyny[68]. Po uzyskaniu dostępu do maszyny pracującej pod systemem Windows zespół ataku może wykorzystać cały wachlarz narzędzi enumeracyjnych. Narzędzia enumeracji domen, takie jak PowerView[69] i BloodHound[70], pozwalają poznawać relacje zaufania zdefiniowane w sieci, umożliwiając eskalację uprawnień pomiędzy kontami użytkowników. Są one często dostępne jako elementy platform *dowodzenia i kierowania* (ang. *command and control*, C2), czyli narzędzi wykorzystywanych po uzyskaniu nieautoryzowanego dostępu (ang. *post-exploitation*). Przykładami platform C2 są CobaltStrike[71] i Empire[72]. Ważne, żeby operatorzy poznali pełen wachlarz możliwości oferowanych przez te i podobne rozwiązania, by nie traktować ich wyłącznie jako narzędzia do przygotowywania szkodliwego oprogramowania wgrywanego na przejmowane komputery albo jako zamkniętych usług zewnętrznych. Zespół ataku powinien być zaznajomiony ze wszystkimi technikami implementowanymi przez używane pakiety oraz mieć umiejętności potrzebne do zastosowania tych samych technik z użyciem innych narzędzi — na wypadek, gdyby zespół obrony zdołał wykryć lub zablokować wykorzystanie głównych pakietów ofensywnych. Istnieją również narzędzia do przeprowadzania enumeracji w aplikacjach webowych oraz do skanowania ich w poszukiwaniu znanych rodzajów podatności na ataki. Zależnie od charakteru konkretnej aplikacji można do jej badania użyć narzędzi takich jak Burp[73], Taipan[74] lub Sqlmap[75]. W trakcie konkursów narzędzia takie służą do wykorzystania luk w zabezpieczeniach aplikacji i wymuszenia wykonania kodu na komputerach przeciwnika, kradzieży danych czy ogólnie przejęcia kontroli nad aplikacją webową. Kolejnym krokiem jest przygotowanie automatyzacji wybranych narzędzi, aby ułatwić ich wykorzystanie operacyjne. Przy czym nie wystarczy tylko przygotować narzędzia przed rozpoczęciem konfliktu — należy jeszcze nauczyć się nimi efektywnie posługiwać. Składnia wywołania tych narzędzi jest zwykle bardzo rozbudowana, więc zdecydowanie polecam w okresie między konfliktami przygotować skrypty lub inne rodzaje automatyzacji, które ułatwią wykonywanie typowych zadań. Na przykład złożone wykonanie narzędzia Nmap można zapisać pod prostym aliasem `turbonmap`:

```
$ alias turbonmap='sudo nmap -sS -Pn --host-timeout=1m --max-rtt-timeout=600ms
↪--initial-rtt-timeout=300ms --min-rtt-timeout=300ms --stats-every 10s
↪--top-ports 500 --min-rate 1000 --max-retries 0 -n -T5 --min-hostgroup 255
↪-oA fast_scan_output -iL'
$ turbonmap 192.168.0.1/24
```

Powyżej przedstawiona metoda skanowania sieci jest bardzo agresywna i generuje dużo ruchu w sieci. Liczba komunikatów może wręcz przytłoczyć i zablokować słabsze domowe rutery, dlatego najważniejsze jest, aby dobrze poznać atakowane środowisko i dostosować do niego proces skanowania. Przyjrzyjmy się niektórym argumentom wywołania, których możesz użyć do dopasowania skali procesu do Twoich potrzeb. Powyższe wywołanie Nmap spowoduje enumerację `500` najczęściej używanych portów TCP (`--top-ports 500`). Narzędzie nie będzie zestawiać pełnych połączeń TCP, lecz jedynie wysyłać początkowe pakiety sygnalizujące chęć nawiązania połączenia (`-sS`), a także zakłada, że wszystkie maszyny z badanego zakresu adresów są

uruchomione (`-Pn`). Powyższe polecenie optymalizuje również całkowity czas wykonania. Przede wszystkim wybrany został szablon ustawień powodujący najszybszą możliwą pracę narzędzia (`-T5`). Następnie zredukowane zostały czasy oczekiwania na uzyskanie pojedynczych rezultatów skanowania (`--max-rtt-timeout=600ms --initial-rtt-timeout=300ms --min-rtt-timeout=300ms`). Wprowadzony też został limit czasu na skanowanie pojedynczej maszyny (`--host-timeout=1m`), wyłączono ponawianie prób skanowania każdego z portów (`--max-retries 0`), ustawiono minimalną liczbę pakietów wysyłanych w ciągu sekundy (`--min-rate 1000`) oraz minimalną liczbę maszyn skanowanych jednocześnie (`--min-hostgroup 255`).

Można także napisać prosty skrypt w Pythonie, który pozwoli stworzyć łańcuch wywołania z wielu narzędzi lub wykonać dogłębniejsze skanowanie. Poniższy przykład pokazuje, jak przeprowadzić początkowe skanowanie przy użyciu narzędzia masscan, a następnie na podstawie uzyskanych wyników przeprowadzić detekcję wersji usług. Zaprezentowana tu logika w dużej mierze została zaczerpnięta z wpisu na blogu Jeffa McJunkina, w którym rozważa on metody skrócenia czasów wykonania rozległych skanowań z użyciem Nmap[76]. W tym przykładzie chciałem pokazać, jak w bardzo prosty sposób można połączyć kilka narzędzi w łańcuch wykonania jedynie za pomocą prostego skryptu powłoki:

```
$ sudo masscan 192.168.0.1/24 -oG initial.gnmap -p 7,9,13,21-23,25-26,37,53,
➥79-81,88,106,110-111,113,119,135,139,143-144,179,199,389,427,443-445,465,
➥513-515,543-544,548,554,587,631,646,873,990,993,995,1025-1029,1110,1433,1720,
➥1723,1755,1900,2000-2001,2049,2121,2717,3000,3128,3306,3389,3986,4899,5000,
➥5009,5051,5060,5101,5190,5357,5432,5631,5666,5800,5900,6000-6001,6646,7070,
➥8000,8008-8009,8080-8081,8443,8888,9100,9999-10000,32768,49152-49157 --rate
➥10000
$ egrep '^Host: ' initial.gnmap | cut -d" " -f2 | sort | uniq > alive.hosts

$ nmap -Pn -n -T4 --host-timeout=5m --max-retries 0 -sV -iL alive.hosts -oA
➥nmap-version-scan
```

Zespół ataku powinien nie tylko umieć użyć podstawowych metod skanowania i wykorzystać odnalezione przypadki podatności na zagrożenia, ale także znać najczęściej wykorzystywane w danym okresie metody przełamywania zabezpieczeń systemów, w szczególności te, które są kierowane przeciwko świeżo ujawnionym publicznie rodzajom podatności (*0-day* lub *n-day*). Oznacza to nie tylko przeprowadzanie skanowania w poszukiwaniu przypadków podatności, ale także przygotowywanie narzędzi do wykorzystywania świeżych luk w oprogramowaniu, dla których istnieją udokumentowane i działające implementacje. Na przykład w kwietniu 2017 roku w wyniku wycieku informacji z NSA doszło do ujawnienia narzędzia EternalBlue — w efekcie upubliczniono przypadek podatności na zagrożenia, który nie został usunięty w wielu organizacjach nawet przez kilka miesięcy lub lat[77]. Przez ten czas publicznie było dostępnych całkiem sporo niestabilnych wersji narzędzi wykorzystujących tę lukę oraz kilka wiarygodnie i stabilnie działających przykładowych implementacji. Zespół czerwony National CCDC przystosował je do ataku na tyle skutecznie, że mieliśmy gotowe skrypty przeprowadzające skanowanie komputerów przeciwników w poszukiwaniu tego rodzaju podatności, zdobywające dostęp do atakowanego urządzenia przy jej użyciu, a następnie wgrywające właściwe szkodliwe oprogramowanie do kontynuowania ataku. Dobrą praktyką jest tworzenie automatycznych skryptów realizujących przełamanie zabezpieczeń systemów przy wykorzystaniu optymalnych argumentów wywołania procedur przełamujących (ang. *exploit*) i gotowych do automatycznego wgrania i uruchomienia na atakowanym urządzeniu narzędzi realizujących kolejny etap ataku. Narzędzia dla kolejnego etapu powinny być

dynamicznie kompilowane dla każdej atakowanej maszyny, więc skrypty automatyzujące operację również powinny to uwzględniać. Niezależna kompilacja dla każdego atakowanego hosta ma na celu ograniczenie możliwości powiązania ze sobą włamań. Najlepiej, gdy procedura przełamująca ładuje narzędzia drugiego etapu bezpośrednio do pamięci operacyjnej, aby uniknąć pozostawiania zbyt wielu śladów dowodowych — sposób realizacji takiego ładowania omówię w kolejnych rozdziałach. Zestaw skryptów do przeprowadzania ataków powinien być dobrze przetestowany na wielu wersjach atakowanych systemów operacyjnych oraz powinien, w razie konieczności, rozpoznawać nieobsługiwane lub niestabilne wersje. Operatorzy uruchamiający skrypt powinni być informowani o możliwym ryzykownym wykonaniu procedur przełamujących, rozumianym jako potencjalnie niestabilne działanie lub działanie wykorzystujące łatwo wykrywalne techniki. W zespołach czerwonych CCDC, aby uniknąć błędów wykonania skryptów wytworzonych własnymi siłami, zazwyczaj wszyscy członkowie są szkoleni w zakresie używania tych narzędzi lub istnieją desygnowani operatorzy legitymujący się odpowiednimi kompetencjami.

Przygotowywanie szkodliwego oprogramowania

Dla każdego zespołu ataku bardzo ważne jest odpowiednie przygotowywanie narzędzi oraz ukrywanie własnej infrastruktury przed przeciwnikiem. Często przygotowywane jest szkodliwe oprogramowanie przeznaczone dla konkretnych atakowanych systemów, więc potrzebne są kompetencje w zakresie używania niskopoziomowych interfejsów systemowych oraz umiejętności programistyczne. W zespole czerwonym National CCDC znaczna część wysiłku programistycznego jest ukierunkowana na przygotowanie elementów szkodliwego oprogramowania instalowanych na atakowanej maszynie, dzięki którym zespół zdobywa dostęp do kolejnych zasobów, uzyskuje trwały nieautoryzowany dostęp, a także może użyć mnóstwa innych funkcjonalności. Na przykład zespół czerwony CCDC posiada narzędzie, które wyłącza lokalne reguły zapory sieciowej, uruchamia wybrane usługi, ukrywa wybrane pliki, a nawet zmienia ustawienia kont użytkowników systemu. Wytwarzanie instalowanych elementów szkodliwego oprogramowania jest kluczowym zagadnieniem dla zespołu ataku, ale często realizowanym zbyt małymi siłami. Osoby obsadzone w tej roli zajmują się wytwarzaniem różnorodnych elementów szkodliwego oprogramowania, od funkcjonalności przeszukiwania i szyfrowania dysku po komponenty realizujące funkcjonalności dowodzenia i kierowania. Na konferencji DEF CON 26 Alex Levinson i ja udostępniliśmy platformę narzędziową Gscript, którą opracowaliśmy dla zespołu czerwonego CCDC[78]. Rozwiązanie to umożliwiało operatorom szybkie zebranie w jednym pakiecie dowolnej liczby już istniejących narzędzi i utajnienie zawartości przez zaciemnienie kodu. Pakiet był kompilowany jako natywnie wykonywalny program w języku Go. Głównym powodem realizacji Gscript była chęć dostarczenia wszystkim członkom zespołu takich samych możliwości szybkiego produkowania instalowanych elementów szkodliwego oprogramowania (implantów) wraz z jednoczesnym udostępnieniem katalogu technik postinfiltracyjnych stosowanych po przełamaniu zabezpieczeń (ang. *post-exploitation*). Bardzo wielką pomocą dla operatorów pracujących z mniej znanym systemem, na przykład OS X lub Windows, jest udostępnienie im sprawdzonych implementacji technik ataku. Dzięki narzędziu Gscript operatorzy mogą także dbać o własne bezpieczeństwo, gdyż zawiera ono funkcjonalności zaciemniania kodu i metody utrudniające zbieranie materiału dowodowego przez obrońców. Każdy, kto przygotowuje szkodliwe oprogramowanie lub inne artefakty przeznaczone do wykorzystania

w atakowanym środowisku, powinien upewnić się, że ich zawartość będzie trudna do odczytania i zrozumienia. Ważne, aby narzędzia służące do ochrony zawartości przesyłanych artefaktów miały możliwość zastosowania metod zaciemniania dla wszystkich rodzajów stosowanych artefaktów. Jeżeli implanty są tworzone w języku Go, to warto przyjrzeć się narzędziu garble[79]. Zapewnia ono dodatkową ochronę programów poprzez usunięcie informacji o procesie kompilacji, zmianę nazw pakietów oraz wyczyszczenie tablic symboli — czyli kolejne kroki *ukrywające rzeczywistość*.

W większości operacji ofensywnych kluczowym komponentem jest infrastruktura dowodzenia i kierowania (C2). Obszar ten jest w zasadzie zupełnie oddzielną dziedziną wiedzy i kompetencji, choć wykorzystywane są w nim implanty wspominane powyżej i często jego utrzymaniem zajmuje się ten sam zespół, który wprowadza szkodliwe oprogramowanie po przełamaniu zabezpieczeń. Zwykle platformy dowodzenia i kierowania oferują ogromną różnorodność funkcjonalności, więc niezmiernie ważne jest dokonanie na etapie planowania wyboru właściwych do zastosowania podczas konkretnej operacji. Główny wybór, jakiego należy dokonać, dotyczy tego, czy oprzeć swoje działania na platformie otwartoźródłowej, czy stworzyć własny tajny zestaw narzędzi. Tworzenie własnych narzędzi z jednej strony może utrudnić obrońcom ich analizę ze względu na brak publicznie dostępnego kodu źródłowego. Z drugiej strony charakterystyczna postać narzędzi może ułatwić zbieranie materiału dowodowego i powiązanie ataków z Twoim zespołem. W zespole czerwonym National CCDC budujemy samodzielnie wiele implantów i platform C2, aby ograniczyć przeciwnikom możliwości analizy publicznie dostępnych źródeł przed rozpoczęciem zawodów. Co prawda korzystamy też z publicznie dostępnych platform, ale przyjmujemy, że mają one niższy poziom bezpieczeństwa operacyjnego ze względu na brak *poufności* kodów źródłowych, więc obrońcy mogą łatwo uzyskać pełen wgląd w wewnętrzną budowę narzędzi, jeżeli je poprawnie zidentyfikują[80]. Bardzo przydatna jest możliwość ładowania dowolnych własnych modułów bezpośrednio do pamięci atakowanej maszyny. Umieściwszy swoje narzędzia w pamięci, utrudniasz obrońcom zapoznanie się z nimi. Przechwycenie takich narzędzi jest możliwe tylko poprzez trwałe zapisanie próbek zawartości pamięci lub poprzez uruchomienie i obserwację szkodliwych modułów w wydzielonym środowisku wirtualnym. Z całą pewnością przydatna będzie funkcjonalność ukrywania komunikacji pomiędzy implantem i serwerem dowodzenia. Programiści platform dowodzenia i kierowania mają bardzo interesujące hobby — wśród protokołów komunikacyjnych używanych przez zwykłe aplikacje wyszukują takie, w których można ukryć własną komunikację, tworząc *skryte kanały komunikacyjne dla dowodzenia i kierowania*. Kandydatami do skrywania agresywnej komunikacji są często protokoły rozbudowanych aplikacji sieciowych, na przykład czaty w czasie rzeczywistym, lub protokoły systemowe udostępniające pola do przesyłania dowolnych danych, takie jak ICMP. Dzięki takiemu maskowaniu swoich komunikatów agresorzy mogą sprawić wrażenie, że ruch sieciowy przez nich generowany jest zupełnie innym, niegroźnym rodzajem ruchu. Zaawansowaną techniką wykorzystującą takie podejście jest *domain fronting* — kiedy prowadzący atak może oszukać rozproszone systemy dostarczania treści (ang. *Content Delivery Network*, CDN), takie jak sieci Tor lub Fastly, i sprawić, że ruch sieciowy będzie dostarczany do infrastruktury atakującego zamiast do zaufanych węzłów sieci CDN. Technicznie sprowadza się to do podania w polu *host* nagłówka protokołu HTTP innej nazwy domenowej, niż była użyta podczas nawiązywania połączenia. W efekcie pakiet po odebraniu go przez sieć CDN jest przekazywany pod adres określony w nagłówku[81]. Omówię dokładniej tę technikę w rozdziale 4., „Nie wyróżniać się z tłumu". Kolejnym tematem do rozważenia jest język programowania używany do tworzenia

implantów. Musisz się zastanowić, czy analityk może łatwo zdekompilować kod implantu lub wręcz odczytać ten kod bezpośrednio z przechwyconej próbki — w takich sytuacjach analitycy obrony mogą w ogóle nie znać się na inżynierii wstecznej, a i tak poznać strukturę szkodliwych narzędzi. Na przykład w przypadku implantów zaprogramowanych w Pythonie lub PowerShellu przeważnie można łatwo cofnąć zaciemnianie kodu i odczytać logikę działania bez konieczności stosowania zaawansowanych technik dekompilacji i dezasemblacji. Nawet oprogramowanie napisane w językach takich jak C# może zostać łatwo zdekompilowane, a jego wewnętrzna struktura zbadana, jeżeli wykorzystano w nim platformę programistyczną .NET. Znakomitą pomocą podczas planowania i wyboru różnych opcji spośród otwartoźródłowych rozwiązań dla dowodzenia i kierowania może być tabela *The C2 Matrix*, podsumowująca wiele nowoczesnych i dostępnych publicznie platform C2[82]. W przykładach opisywanych w książce będę się posługiwał przede wszystkim rozwiązaniem Sliver — platformą C2 napisaną w języku Go[83]. Jeszcze raz powtórzę, że wykorzystanie funkcjonalności zaciemniania kodu implantu będzie podstawą spowalniania analiz prowadzonych przez zespół obrony. Rzeczą wartą rozważenia podczas planowania infrastruktury dowodzenia i kierowania jest możliwość jednoczesnego wykonywania wielu prób zainfekowania atakowanej sieci z wykorzystaniem różnych platform C2. Dzięki wykorzystywaniu różnych implantów, o różnych tempach komunikacji zwrotnej i różnych zakresach zwrotnych adresów IP, możesz lepiej chronić implanty przed wykryciem i utrudniasz ich powiązanie ze sobą. Czasem warto zupełnie rozdzielić od siebie całe grupy implantów i platformy nimi zarządzające, aby ujawnienie jednej z nich nie powodowało ujawnienia kolejnej. A czasami warto nawet zainfekować jedną maszynę wieloma niezależnymi implantami, tak że nawet jeżeli część z nich zostanie wykryta i usunięta, to nieautoryzowany dostęp do urządzenia pozostanie aktywny. Często stosowaną strategią jest bieżące wykorzystywanie tylko jednego z tych implantów i trzymanie pozostałych w odwodzie dla zapewnienia długofalowego utrzymania nieautoryzowanego dostępu. W przypadku gdy połączenie z głównym narzędziem zostanie utracone, zawsze można uruchomić któryś z pozostałych uśpionych implantów. W zespole czerwonym CCDC często wykorzystujemy do tego celu rozwiązania takie jak CobaltStrike i Metasploit, umożliwiające między innymi współpracę członków zespołu. Zwykle operatorów zawiadujących grupowymi i zapasowymi infrastrukturami dowodzenia i kierowania nazywamy *przewodnikami po powłokach*, bo prowadzą innych członków zespołu do utraconych połączeń.

Narzędzia pomocnicze

Serwer do łamania skrótów kryptograficznych na pewno ułatwi zespołowi poszerzanie dostępu do atakowanego środowiska. Często taki element infrastruktury jest postrzegany jako nieistotny, ale w praktyce może bardzo usprawnić działania operacyjne zespołu ataku. Niewątpliwie podczas przeszukiwania atakowanego środowiska zespół napotka różnego rodzaju utajnione informacje — zaszyfrowane lub pod postacią skrótów kryptograficznych. Rozszyfrowanie tych informacji będzie konieczne dla uzyskania dostępu do kolejnych elementów atakowanej infrastruktury. Uruchamiając rozwiązanie deszyfrujące, zwiększasz bezpieczeństwo operacyjne prowadzonych działań oraz zyskujesz możliwość wybierania, na których informacji rozszyfrowanie przeznaczyć więcej zasobów. Znakomitym przykładem rozwiązania zarządzającego infrastrukturą łamania szyfrów jest CrackLord[84]. Przy okazji uruchamiania tej infrastruktury warto przygotować w łatwo dostępnej lokalizacji zestaw tęczowych tablic i listy słów — te proste koncepcyjnie elementy mogą wydatnie zwiększyć wydajność odgadywania haseł i enumeracji. Jeżeli masz odpowiednio

dużą wiedzę na temat atakowanego środowiska, to warto przygotować przeznaczone dla niego listy słów oparte na słownictwie typowym dla atakowanej firmy lub konkurencyjnego zespołu. Uważam, że bardzo przydatne do tego celu jest narzędzie CeWL, które pozwala przeprowadzić enumerację serwisów sieciowych i na podstawie ich treści przygotować listy słów[85]. Podobnie jak w przypadku infrastruktury obrony, bardzo przydatne są współdzielone usługi transformacji danych. Zespół ataku może też wiele skorzystać na posługiwaniu się rozwiązaniami takimi jak CyberChef lub PFM, ponieważ z atakowanego środowiska także pozyskiwanych jest wiele artefaktów, które trzeba następnie przeanalizować. Strona ofensywna może nawet wykorzystać technologię podobną do rozwiązań SIEM, aby indeksować i porządkować dane pozyskane z atakowanej sieci. Udostępnienie całemu zespołowi ataku współdzielonych narzędzi pomocniczych, takich jak serwer łamania haseł lub usługi transformacji danych, podobne do CyberChef, wiąże się z pewnym początkowym kosztem — ale jest to cena, którą warto zapłacić za zwiększenie wydajności operacyjnej.

Na koniec warto wspomnieć o infrastrukturze raportowej, prawdopodobnie kompletnie niedocenianej w większości zespołów ofensywnych. Niezależnie od tego, czy zespół pracuje nad prawdziwym zadaniem ofensywnym, czy bierze udział w konkursie podobnym do CCDC, konieczny jest sposób prezentowania postępów prac. W trakcie konkursów CCDC lub Pros V Joes punktacja jest zliczana na podstawie zmierzonej niedostępności usług chronionych przez zespół obrony oraz na podstawie liczby udanych włamań zgłoszonych przez zespół ataku. Pomiar punktów obrony jest realizowany przez automatycznego agenta punktacyjnego, który regularnie sprawdza, czy usługi reagują prawidłowo na zlecenia. Po stronie ataku zespół ma udostępniony serwer raportowy, przy za pomocą którego dokumentowane są udane włamania wraz z wykradzionymi danymi i dowodami przełamania zabezpieczeń. Podobne serwery z dokumentacją pomyślnych włamań występują też w trakcie prawdziwych operacji ofensywnych i mogą przyjmować różnorodne postaci, od serwera dowodzenia i kierowania zarządzającego botnetem po zaawansowaną aplikację prezentującą przychody całej organizacji i poszczególnych jej członków. Nasze serwery raportujące używane w trakcie zawodów ewoluowały przez lata i obecnie dane o włamaniach prezentowane są na skomplikowanych panelach raportowych. Powstały także narzędzia wspomagające formatowanie danych oraz automatycznie dokumentujące włamania. To może nie być początkowo najbardziej istotna kwestia, ale w pewnym momencie warto rozważyć wprowadzenie jakiegoś stopnia automatyzacji raportowania, aby zaoszczędzić czas później.

Wprawdzie można wykorzystywać zestaw wielu popularnych narzędzi dla zespołów czerwonych dostarczanych wraz z dystrybucją Linux Kali[86] analogicznie do wykorzystania narzędzia Security Onion 2, ale nie polecam używania ich do podstawowych działań operacyjnych. Myślę, że system Kali całkiem nieźle sprawdziłby się w niektórych scenariuszach konkursowych, lecz do prawdziwych operacji ofensywnych raczej używaj samodzielnie wykonanych narzędzi. Podobnie raczej nie należy stosować rozwiązania Security Onion 2 do wszystkiego, łatwiej będzie przygotować zestaw wyselekcjonowanych narzędzi w specjalnie do tego celu założonym repozytorium lub na dedykowanych obrazach systemów. Niemniej trzeba przyznać, że dystrybucja systemu Kali sprawdza się doskonale przy poznawaniu rozmaitych narzędzi i eksperymentowaniu z różnymi rozwiązaniami. Polecam stworzyć własne repozytorium skryptów i narzędzi, które wykorzystuje Twój zespół. W ten sposób będzie można je łatwo utrzymywać i wgrywać do dowolnie wybranego obrazu systemu. Przy wykorzystaniu takiego repozytorium można łatwo utrzymywać spójność między zbiorem narzędzi a używanymi przez operatorów wersjami poddanymi

procedurom zaciemniania kodu i ukrywania wewnętrznej struktury. W ten sposób możliwe jest łagodzenie skutków usterek istniejących w podstawowych wersjach używanych systemach operacyjnych oraz zapewnienie dodatkowego poziomu bezpieczeństwa operacyjnego przez ukrycie budowy wewnętrznej podstawowego zestawu narzędzi.

Kluczowe wskaźniki efektywności zespołu ataku

Kluczowe wskaźniki efektywności są dobrym narzędziem do pomiaru efektywności działań Twojego zespołu i jej zmian w czasie. Przy czym warto zauważyć, że inaczej niż w przypadku zespołów obrony, wskaźniki dobrze pokazujące efektywność zespołu konkursowego raczej nie będą się sprawdzać w przypadku zespołu testów penetracyjnych lub zespołu czerwonego na stałe pracującego w organizacji. Wynika to przede wszystkim z odmiennych podstawowych celów stojących przed zespołem konkursowym i typowymi zespołami weryfikującymi zabezpieczenia — ich celem finalnie jest pomóc klientowi poprawić zabezpieczenia systemów, a nie utrzymywać nieautoryzowany dostęp do systemów przy jednoczesnym ukrywaniu się. W przypadku zespołu czerwonego National CCDC dobrze jest wiedzieć, jak radzą sobie w każdym roku nasze lokalne zespoły, więc zbieramy i przechowujemy szczegółowe dane pomiarowe o wynikach działań każdego operatora i przechowujemy stworzone na podstawie tych danych raporty, aby móc porównywać różnice rok do roku. Zebrane dane wykorzystujemy też do porównywania metod dokonywania włamań komputerowych oraz do identyfikowania słabych i silnych stron naszego zespołu czerwonego. Pośród wskaźników, jakie zbieramy, najbardziej interesujące to średni czas potrzebny na uruchomienie infrastruktury ofensywnej, czas potrzebny do zainfekowania kolejnych elementów infrastruktury po pomyślnym początkowym przełamaniu zabezpieczeń na jednej maszynie (ang. *breakout time*), średni czas utrzymywania nieautoryzowanego dostępu do atakowanego środowiska (ang. *persistence time*), średnia liczba zinfiltrowanych maszyn (wyrażona jako wartość procentowa całkowitej liczby maszyn), średnia liczba zdobytych punktów, średnia długość raportu. Oczywiście przechowujemy także szczegółowe informacje o każdej udanej infiltracji. Nie wszystkie wartości są mierzone i zapisywane automatycznie — część wyliczamy na podstawie ręcznie wprowadzanych raportów o infiltracjach, a część, jak na przykład czas potrzebny do zainfekowania kolejnych elementów infrastruktury, po prostu wprowadzamy ręcznie. Niemniej wartości tych wskaźników pozwalają nam zidentyfikować obszary, nad którymi powinniśmy popracować pomiędzy rozgrywkami, oraz dostrzec obszary, w których udało się nam zrobić wymierne postępy.

Podsumowanie

W tym rozdziale omówiłem podstawowe pojęcia dotyczące planowania działań oraz przedstawiłem kluczowe technologie, które każda ze stron konfliktu powinna postarać się wdrożyć przed rozpoczęciem cyberkonfliktu. Przedstawiłem elementy infrastruktury przydatne obu zespołom, takie jak narzędzia wiki do współdzielenia wiedzy czy różnego rodzaju komunikatory i czaty usprawniające komunikację zespołową i prowadzenie operacji. Omówiłem wybrane strategie planowania długofalowego, między innymi tworzenie i rozwój zespołu prowadzącego cyberoperacje oraz przygotowywanie planów alternatywnych i zapasowych narzędzi. Opisałem obszary

kompetencji, które powinny istnieć wśród członków każdego z zespołów w cyberkonflikcie, a także metody systematycznego podwyższania kwalifikacji członków zespołu. Zgłębiłem też zagadnienia związane z ogólnym planowaniem operacyjnym, planowaniem uczestnictwa w konkretnym konflikcie oraz doskonaleniem działań operacyjnych. Pokazałem, jak istotne jest dokonywanie pomiarów przy użyciu wskaźników jakości, gdyż umożliwia to obserwację rozwoju zespołu — wskazałem również przykładowe wartości, które mogą być mierzone zarówno w zespole ataku, jak i obrony. Omówiłem całkiem sporo strategii obronnych oraz elementów infrastruktury, które obrońcy powinni przygotować przed rozpoczęciem cyberkonfliktu. W treści rozdziału zamieściłem opisy różnorodnych form zbierania danych bezpieczeństwa, obejmujących pomiary i obserwacje wykonywane w ramach pojedynczego urządzenia, w ramach sieci komputerowej lub w obrębie aplikacji. Pobieżnie przedstawiłem kwestię aktywnej infrastruktury obronnej w postaci serwerów pułapek — wrócę do niej w kolejnych rozdziałach. Następnie zająłem się tematami zarządzania danymi obronnymi, od zbierania i katalogowania powiadomień i alertów w rozwiązaniach SIEM, przez wzbogacanie zebranych informacji za pomocą aplikacji SOAR, po niezliczone narzędzia, które nie są niezbędne do skutecznego działania, ale bardzo ułatwiają aktywności z użyciem aplikacji SOAR. Omówiłem także metody tworzenia alertów z wbudowaną logiką działania oraz zarządzanie definicjami alertów. Wymieniłem wiele platform narzędziowych, które zespół obrony może wykorzystać, aby ułatwić zarządzanie infrastrukturą. W dalszej kolejności przedstawiłem narzędzia analityczne typowo wykorzystywane przez zespoły cyberobrony, na przykład narzędzia informatyki śledczej, takie jak The Sleuth Kit. Na przykładzie narzędzia BLUESPAWN pokazałem, jak wprowadzanie innowacji i tworzenie własnych narzędzi analitycznych może zwiększyć przewagę obrońców nad przeciwnikami. Temat innowacji będzie powracał w całej książce — jeszcze nie raz zamierzam pokazać, jak można uzyskać przewagę nad przeciwnikiem, wprowadzając innowacje często bardzo proste koncepcyjnie.

W dalszej części rozdziału przedstawiłem ogólne cele i taktyki charakterystyczne dla strony ofensywnej. Zespół ataku ma do dyspozycji szeroki wachlarz narzędzi do przeprowadzania skanowania i enumeracji infrastruktury przeciwnika, dzięki czemu możliwe jest sprawdzenie rodzajów i wersji zainstalowanych elementów infrastruktury, a następnie dobranie odpowiednich metod infiltracji. Pokazałem, że szybko działające zespoły, takie jak zespół czerwony CCDC, zwykle mają zawczasu przygotowane i zautomatyzowane odpowiednie narzędzia infiltracyjne, dzięki czemu zyskują nie tylko szybkość, ale też powtarzalność działań. Zagłębiłem się w kwestię przygotowywania szkodliwego oprogramowania dostarczanego do zinfiltrowanych systemów. W szczególności pokazałem, że zespół ataku musi podjąć szereg świadomych i rozważnych decyzji, jeżeli chodzi o metody tworzenia implantów i organizację architektury dowodzenia i kierowania. Opisałem także narzędzia pomocnicze przeznaczone dla zespołu ataku, takie jak serwery do łamania kryptografii, serwery raportowe czy aplikacje do współdzielenia i współprzetwarzania danych.

Na koniec omówiłem wskaźniki wydajności dla zespołów ataku pozwalające w mierzalny sposób weryfikować zmiany w skuteczności zespołu podczas konkursów cyberbezpieczeństwa. W kolejnym rozdziale przedstawię szczegółowo konkretne techniki realizacji skutecznych ataków na infrastrukturę wraz z optymalnymi metodami odpowiedzi strony przeciwnej. W szczególności zajmę się tematem pamięci operacyjnej systemów: dlaczego jej wykorzystanie jest takie ważne i jak obrona może przeciwdziałać temu wykorzystaniu, zwiększając widoczność poczynań agresora.

Źródła

[1] Aplikacja umożliwiająca jednoczesną pracę grupową nad tworzonymi notatkami, którą można zainstalować w obrębie własnej infrastruktury, *Etherpad-lite*, *https://github.com/ether/etherpad-lite*, [dostęp: 7 października 2021].

[2] Proste rozwiązanie otwartoźródłowe do tworzenia dokumentacji wiki, zawiera obsługę szablonów i dołączanych modułów oraz posiada zintegrowane mechanizmy uwierzytelniania, *Dokuwiki*, *https://github.com/splitbrain/dokuwiki*, [dostęp: 7 października 2021].

[3] EKM (Enterprise Key Management), funkcjonalność pakietu Slack oferująca organizacjom szyfrowanie przesyłanych wiadomości i rejestrowanych danych przy użyciu własnych kluczy kryptograficznych, *https://slack.com/enterprise-key-management*, [dostęp: 7 października 2021].

[4] Chase Melissa, Perrin Trevor, Zaverucha Greg, *The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption*, 2019, *https://signal.org/blog/pdfs/signal_private_group_system.pdf*, [dostęp: 7 października 2021].

[5] St-Pierre Georges, Kingsley Justin, *Professional fighter Georges St-Pierre on the importance of innovation*, *https://www.theglobeandmail.com/report-on-business/careers/careers-leadership/professional-fighter-georges-st-pierre-on-the-importance-of-innovation/article11891399/#*, [dostęp: 7 października 2021].

[6] Katalog płatnych kursów online z obszaru cyberbezpieczeństwa instytutu SANS, *https://www.sans.org/online-security-training/*, [dostęp: 7 października 2021].

[7] Katalog wysokiej jakości darmowych szkoleń na temat bezpieczeństwa informacji Open Security Training, *https://opensecuritytraining.info/Training.html*, [dostęp: 7 października 2021].

[8] Biblioteka darmowych kursów z bezpieczeństwa informacji, zorganizowana w podziale na ścieżki rozwoju zawodowego, *Cybrary*, *https://app.cybrary.it/browse/refined?view=careerPath*, [dostęp: 7 października 2021].

[9] Meyers Adam, *First-Ever Adversary Ranking in 2019 Global Threat Report Highlights the Importance of Speed*, 2019, *https://www.crowdstrike.com/blog/first-ever-adversary-ranking-in-2019-global-threat-report-highlights-the-importance-of-speed/*, [dostęp: 7 października 2021].

[10] *OSQuery*, *https://github.com/osquery/osquery*, [dostęp: 7 października 2021].

[11] Rozwiązanie EDR przeznaczone dla systemów Windows, Linux i macOS, dystrybuowane jako open source, *GRR*, *https://github.com/google/grr*, [dostęp: 7 października 2021].

[12] Rozwiązanie EDR przeznaczone dla systemów Windows, Linux i macOS, dystrybuowane jako open source, stanowiące rozwinięcie narzędzi wytworzonych w ramach projektu OSSEC, *Wazuh*, *https://github.com/wazuh/wazuh*, [dostęp: 7 października 2021].

[13] Rozwiązanie EDR przeznaczone dla systemów Windows, Linux i macOS, dystrybuowane jako open source, inspirowane narzędziami GRR i OSQuery, *Velociraptor*, *https://github.com/Velocidex/velociraptor*, [dostęp: 7 października 2021].

[14] Podręcznik użytkownika narzędzia Snort, systemu wykrywania włamań (IDS), dla platform Windows i Linux, dystrybuowanego jako open source, *http://manual-snort-org.s3-website-us-east-1.amazonaws.com/*, [dostęp: 7 października 2021].

[15] Opis narzędzia Suricata, wielowątkowego systemu wykrywania i zapobiegania włamaniom dla platformy Linux, dystrybuowanego jako open source, *https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata*, [dostęp: 7 października 2021].

[16] Dokumentacja narzędzia Zeek, systemu wykrywania włamań (IDS), umożliwiającego rejestrowanie zdarzeń i wartości wskaźników różnych protokołów sieciowych, powstałego na bazie narzędzia Bro IDS, *https://docs.zeek.org/en/master/*, [dostęp: 7 października 2021].

[17] Ehrlich Yoram, *Port Mirroring for Network Monitoring Explained*, *https://blog.niagaranetworks.com/blog/port-mirroring-for-network-monitoring-explained*, [dostęp: 7 października 2021].

[18] Fortuna Andrea, *TCPDUMP: A simple cheatsheet*, *https://www.andreafortuna.org/2018/07/18/tcpdump-a-simple-cheatsheet/*, [dostęp: 7 października 2021].

[19] Dokumentacja narzędzia Wireshark — wprowadzenie, *What is Wireshark?*, *https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs*, [dostęp: 7 października 2021].

[20] Dokumentacja platformy programistycznej narzędzia Wireshark, umożliwiającej definiowanie własnych modułów interpretacji nowych protokołów sieciowych, *Adding a basic dissector*, *https://www.wireshark.org/docs/wsdg_html_chunked/ChDissectAdd.html*, [dostęp: 7 października 2021].

[21] Brenton Chris, *Tshark Examples — Theory & Implementation*, *https://www.activecountermeasures.com/tshark-examples-theory-implementation/*, [dostęp: 7 października 2021].

[22] Johnson Josh, *Implementing Active Defense Systems on Private Networks*, *https://www.sans.org/reading-room/whitepapers/detection/implementing-activedefense-systems-private-networks-34312*, [dostęp: 7 października 2021].

[23] *Filebeat — A lightweight logging application*, *https://www.elastic.co/beats/filebeat*, [dostęp: 7 października 2021].

[24] *Configure Computers to Forward and Collect Events*, *https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc748890(v=ws.11)*, [dostęp: 7 października 2021].

[25] Narzędzie przeznaczone do wykrywania anomalii w aktywności użytkowników, *Splunk: User Behavior Analytics*, *https://www.splunk.com/en_us/software/user-behavior-analytics.html*, [dostęp: 7 października 2021].

[26] *HELK, The Threat Hunter's Elastic Stack*, *https://github.com/Cyb3rWard0g/HELK*, [dostęp: 7 października 2021].

[27] *The Elastic Stack*, *https://www.elastic.co/elastic-stack*, [dostęp: 7 października 2021].

[28] Narzędzie SIEM do przetwarzania danych sieciowych, *VAST*, *https://github.com/tenzir/vast*, [dostęp: 7 października 2021].

[29] Aplikacja SOAR współpracująca z TheHive, *Cortex*, *https://github.com/TheHive-Project/Cortex*, [dostęp: 7 października 2021].

[30] *TALR — Threat Alert Logic Repository*, *https://github.com/SecurityRiskAdvisors/TALR*, [dostęp: 7 października 2021].

[31] Definicja formatu powiadomień z wykorzystaniem logiki kombinatorycznej, *OpenIOC*, *https://github.com/mandiant/OpenIOC_1.1*, [dostęp: 7 października 2021].

[32] *COPS — Collaborative Open Playbook Standard*, *https://github.com/demisto/COPS*, [dostęp: 7 października 2021].

[33] *ElastAlert — Easy & Flexible Alerting With Elasticsearch*, *https://elastalert.readthedocs.io/en/latest/elastalert.html*, [dostęp: 7 października 2021].

[34] System zarządzania powiadomieniami i alertami, *TheHive*, *https://github.com/TheHive-Project/TheHive*, [dostęp: 7 października 2021].

[35] *MISP — Threat Intelligence Sharing Platform*, *https://github.com/MISP/MISP*, [dostęp: 7 października 2021].

[36] Zestaw skryptów open source w Pythonie do zarządzania wiedzą na temat zagrożeń, *CRITS*, *https://github.com/crits/crits/wiki*, [dostęp: 7 października 2021].

[37] Zestaw zaawansowanych narzędzi systemowych dla systemu Windows, zawiera wiele funkcji i narzędzi przydatnym przy reagowaniu na incydenty, *Windows Sysinternals*, *https://docs.microsoft.com/en-us/sysinternals/*, [dostęp: 7 października 2021].

[38] *YARA in a nutshell*, *https://virustotal.github.io/yara/*, [dostęp: 7 października 2021].

[39] Narzędzie do zautomatyzowanej ekstrakcji artefaktów, *Binwalk*, *https://github.com/ReFirmLabs/binwalk*, [dostęp: 7 października 2021].

[40] Narzędzie do ukierunkowanej ekstrakcji artefaktów, *Scalpel*, *https://github.com/sleuthkit/scalpel*, [dostęp: 7 października 2021].

[41] Baza wiedzy o taktykach ataków MITRE ATT&CK, *Compromise Application Executable*, *https://attack.mitre.org/techniques/T1577/*, [dostęp: 7 października 2021].

[42] Darmowy produkt firmy FireEye, umożliwiający przechwytywanie i analizę zawartości pamięci systemu Windows, *Redline*, *https://www.fireeye.com/services/freeware/redline.html*, [dostęp: 7 października 2021].

[43] Pakiet open source do przeprowadzania analiz śledczych na obrazach dysków, *The Sleuth Kit*, *https://www.sleuthkit.org/*, [dostęp: 7 października 2021].

[44] Pakiet narzędziowy do ekstrakcji zawartości pamięci operacyjnej systemów komputerowych, *Volatility Framework*, *https://github.com/volatilityfoundation/volatility*, [dostęp: 7 października 2021].

[45] Pakiet narzędzi dla zespołów obrony oferujący funkcjonalności podwyższania bezpieczeństwa systemów, poszukiwania przypadków podatności na zagrożenia i monitorowania, *BLUESPAWN*, *https://github.com/ION28/BLUESPAWN*, [dostęp: 7 października 2021].

[46] Smith Jake, McDowell Jack, Konferencja DEFCON edycja 28, *BLUESPAWN: An open-source active defense and EDR solution*, *https://github.com/ION28/BLUESPAWN/blob/master/docs/media/Defcon28-BlueTeamVillage-BLUESPAWN-Presentation.pdf*, [dostęp: 7 października 2021].

[47] Narzędzie do poszukiwania szkodliwego oprogramowania w pamięci operacyjnej, *PE-Sieve*, *https://github.com/hasherezade/pe-sieve*, [dostęp: 7 października 2021].

[48] Zaprogramowana w Pythonie platforma przechowywania i automatycznej analizy artefaktów, *Viper*, *https://github.com/viper-framework/viper*, [dostęp: 7 października 2021].

[49] Dynamiczne wydzielone środowisko uruchomieniowe umożliwiające prowadzenie badania plików wykonywalnych w trakcie pracy, *Cuckoo Sandbox*, *https://github.com/cuckoosandbox/cuckoo*, [dostęp: 7 października 2021].

[50] Pakiet do zautomatyzowanej instalacji narzędzia Cuckoo Sandbox, *BoomBox*, *https://github.com/nbeede/BoomBox*, [dostęp: 7 października 2021].

[51] Symulator ruchu sieciowego współpracujący z wydzielonymi środowiskami uruchomieniowymi, *INetSim*, *https://github.com/catmin/inetsim*, [dostęp: 7 października 2021].

[52] Aplikacja online do przeprowadzania podstawowych analiz statycznych wprowadzonego pliku wraz z analizą antywirusową i analizą informacji o znanych zagrożeniach, *VirusTotal*, *https://www.virustotal.com/gui/*, [dostęp: 7 października 2021].

[53] Komercyjne rozwiązanie oferujące dostęp do wydzielonych środowisk uruchomieniowych, *JoeSecurity*, *https://www.joesecurity.org/*, [dostęp: 7 października 2021].

[54] Darmowe wydzielone środowisko uruchomieniowe dla plików wykonywalnych systemu Windows, *ANY.RUN*, *https://any.run/*, [dostęp: 7 października 2021].

[55] Częściowo darmowe wydzielone środowisko uruchomieniowe, *Hybrid Analysis*, *https://www.hybrid-analysis.com/*, [dostęp: 7 października 2021].

[56] Aplikacja open source do współdzielenia i przetwarzania danych, *CyberChef*, *https://github.com/gchq/CyberChef*, [dostęp: 7 października 2021].

[57] Napisana w Pythonie aplikacja open source do transformacji danych, *Pure Funky Magic*, *https://github.com/mari0d/PFM*, [dostęp: 7 października 2021].

[58] Dokumentacja systemu Maltego, *What is Maltego?*, *https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-*, [dostęp: 7 października 2021].

[59] Lambert Wes, wystąpienie na konferencji GrayHat 2020, *Security Onion — Unravel Adversary Actions with Frighteningly Good Detection and Shocking Visibility*, *https://www.youtube.com/watch?v=M-ty0o8dQU8*, [dostęp: 7 października 2021].

[60] Tunggal Abi Tyas, *14 Cybersecurity Metrics + KPIs to Track*, *https://www.upguard.com/blog/cybersecurity-metrics*, [dostęp: 7 października 2021].

[61] Perez Carloz, *Are we measuring Blue and Red Right?*, *https://www.darkoperator.com/blog/2015/11/2/are-we-measuring-blue-and-red-right*, [dostęp: 7 października 2021].

[62] Lambert John, wpis na Twitterze na temat prowadzenia badań technik ofensywnych, *https://twitter.com/johnlatwc/status/442760491111178240*, [dostęp: 7 października 2021].

[63] Zautomatyzowane narzędzia skanujące, *AutoRecon*, *https://github.com/Tib3rius/AutoRecon*, [dostęp: 7 października 2021].

[64] Rozproszone rozwiązanie skanujące z interfejsem webowym, *Scantron*, *https://github.com/rackerlabs/scantron*, [dostęp: 7 października 2021].

[65] Moduł skanowania dla narzędzia nmap umożliwiający poszukiwanie przypadków podatności na zagrożenia, *nmap vulners*, *https://github.com/vulnersCom/nmap-vulners*, [dostęp: 7 października 2021].

[66] Rozwiązanie open source do skanowania w poszukiwaniu przypadków podatności na zagrożenia, *OpenVAS*, *https://github.com/greenbone/openvas*, [dostęp: 7 października 2021].

[67] Modularny pakiet open source do przeprowadzania skanowania, infiltracji i działań postinfiltracyjnych, *Metasploit*, *https://github.com/rapid7/metasploit-framework*, [dostęp: 7 października 2021].

[68] Zestaw skryptów automatyzujących korzystanie z pakietu Metasploit, obejmujących także działania postinfiltracyjne, *Metasploit Resource Scripts*, *https://docs.rapid7.com/metasploit/resource-scripts/*, [dostęp: 7 października 2021].

[69] *PowerView*, *https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon*, [dostęp: 7 października 2021].

[70] Narzędzie do odczytu danych o domenach Windows i budowania map ich relacji zaufania w grafowej bazie danych, *BloodHound*, *https://github.com/BloodHoundAD/BloodHound*, [dostęp: 7 października 2021].

[71] Popularna platforma dowodzenia i kierowania, zawierająca graficzny interfejs użytkownika i język skryptowy Aggressor Script, *CobaltStrike*, *https://www.cobaltstrike.com/*, [dostęp: 7 października 2021].

[72] Popularna platforma open source dowodzenia i kierowania, współpracująca z systemami Windows i macOS, zawiera wiele funkcjonalności postinfiltracyjnych, *Empire*, *https://github.com/BC-SECURITY/Empire*, [dostęp: 7 października 2021].

[73] Aplikacja pośrednicząca w komunikacji z aplikacjami webowymi, oferuje wersję darmową i wersję komercyjną z dodatkowymi funkcjonalnościami, *Burp Suite*, *https://portswigger.net/burp*, [dostęp: 7 października 2021].

[74] Skaner podatności w aplikacjach webowych, dostępne są wersja społecznościowa i wersja komercyjna, *Taipan*, *https://taipansec.com/index*, [dostęp: 7 października 2021].

[75] Zautomatyzowany skaner podatności, głównie związanej ze wstrzykiwaniem kodu SQL, *Sqlmap*, *https://github.com/sqlmapproject/sqlmap*, [dostęp: 7 października 2021].

[76] McJunkin Jeff, wpis na blogu na temat pomiaru wydajności narzędzia Nmap i jej poprawy z użyciem narzędzia Masscan, *https://jeffmcjunkin.wordpress.com/2018/11/05/masscan/*, [dostęp: 7 października 2021].

[77] Wikipedia, *EternalBlue*, *https://en.wikipedia.org/wiki/EternalBlue*, [dostęp: 7 października 2021].

[78] Napisane w języku Go narzędzie służące do wgrywania szkodliwego oprogramowania na różne platformy systemowe, *Gscript*, *https://github.com/gen0cide/gscript*, [dostęp: 7 października 2021].

[79] Napisane w języku Go narzędzie do zaciemniania kodu, *garble*, *https://github.com/burrowers/garble*, [dostęp: 7 października 2021].

[80] Wikipedia, *Operations security*, *https://en.wikipedia.org/wiki/Operations_security*, [dostęp: 7 października 2021].

[81] Fat Rodzianko, wpis na blogu dotyczący stosowania techniki domain fronting w sieci Azure, *https://fatrodzianko.com/2020/05/11/covenant-c2-infrastructure-with-azure-domain-fronting/*, [dostęp: 7 października 2021].

[82] Porównanie funkcjonalności otwartoźródłowych platform dowodzenia i kierowania, *The C2 Matrix*, *https://www.thec2matrix.com/matrix*, [dostęp: 7 października 2021].

[83] Otwartoźródłowa platforma dowodzenia i kierowania, *Sliver*, *https://github.com/BishopFox/sliver*, [dostęp: 7 października 2021].

[84] Napisana w języku Go aplikacja do zarządzania zadaniami łamania skrótów kryptograficznych, *Cracklord*, *https://github.com/jmmcatee/cracklord*, [dostęp: 7 października 2021].

[85] Generator list słów, *CeWL*, *https://github.com/digininja/CeWL*, [dostęp: 7 października 2021].

[86] Dystrybucja systemu Linux zawierająca zestaw ofensywnych narzędzi cyberbezpieczeństwa, *Kali Linux*, *https://www.kali.org/*, [dostęp: 7 października 2021].

Przygotuj się. Cyberwojna nadchodzi!

Cyfrowe konflikty stały się codziennością. Organizacja, która chce przetrwać w tym wrogim świecie, nie może szczędzić sił ani środków na cyberbezpieczeństwo. Napastnicy prowadzą wyrafinowane ataki z rosnącą skutecznością. Nawet jeśli Twój system komputerowy jest dobrze zabezpieczony, a procedury cyberbezpieczeństwa zostały wdrożone i są stosowane, musisz się przygotować do ataku. Innymi słowy: musisz dobrze wiedzieć, co robić, kiedy prawdziwi hakerzy wtargną do Twojego systemu.

Ta niezwykła książka pozwoli Ci dobrze zrozumieć, jak wygląda prowadzenie cyberataku z perspektywy agresora i odpieranie napaści z perspektywy obrońcy. Znajdziesz w niej mnóstwo przydatnych porad i wskazówek, dzięki którym zdołasz przejąć kontrolę nad sytuacją. Opisane tu techniki i sztuczki okazują się przydatne podczas całego łańcucha ataku. W każdym rozdziale poruszono tematy ważne dla zespołów ataku lub zespołów obrony. Pokazano świat antagonistycznych operacji, a także zasady oszustwa, człowieczeństwa i ekonomii, będące podstawą prowadzenia konfliktów komputerowych. Przedstawiono wszelkie niezbędne informacje dotyczące planowania operacji, instalacji infrastruktury i narzędzi. Omówiono również zalety prowadzenia zaawansowanych badań i wyciągania wniosków z zakończonych konfliktów.

W książce między innymi:

- wstrzykiwanie kodu do procesów i wykrywanie wstrzykniętego kodu
- aktywne środki obrony
- manipulacja sensorami obrońców podczas ataku
- wprowadzanie tylnych drzwi do programów i używanie serwerów-pułapek
- techniki stosowane w czerwonych i niebieskich zespołach
- najlepsze metody pozwalające wygrać konflikt cyberbezpieczeństwa

Dan Borges

jest programistą specjalizującym się w zagadnieniach bezpieczeństwa. Zajmował się między innymi testami penetracyjnymi, symulacją ataków, a także analizami w operacyjnych centrach bezpieczeństwa. Przez osiem lat był członkiem czerwonego zespołu w konkursie National Collegiate Cyber Defense Competition, a przez pięć lat prowadził konkurs Global Collegiate Penetration Testing Competition.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-8684-6
9 788328 386846
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 79,00 zł
Packt