PRZEGLĄD TELEINFORMATYCZNY
NR 1-2, 2017

Metodyka szkoleń w zakresie ochrony aplikacji internetowych przed atakami z cyberprzestrzeni

Krystian WOJDYGOWSKI, Zbigniew ŚWIERCZYŃSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
krystian.wojdygowski@wat.edu.pl, zbigniew.swierczynski@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono założenia autorskiej metodyki przeprowadzenia szkoleń z zakresu ochrony aplikacji internetowych przed atakami z cyberprzestrzeni. Oprócz metodyki, opisano stanowisko laboratoryjne opracowane specjalnie na potrzeby realizacji części praktycznej metodyki. Przedstawiono przykładowe scenariusze zadań szkoleniowych, co z punktu widzenia dydaktycznego stanowi spójną całość i umożliwia przekazywanie wiedzy w sposób kompleksowy, usystematyzowany oraz dobrze przyswajalny przez odbiorców.

SŁOWA KLUCZOWE: bezpieczeństwo aplikacji internetowych (WWW), cyberbezpieczeństwo, zapora sieciowa warstwy aplikacji

1. Wprowadzenie

Rozwój nowych technologii oraz ich upowszechnianie przyczynia się jednocześnie do zwiększenia popularności aplikacji internetowych, a tym samym do ciągłego ich rozwoju, aby sprostać nowym potrzebom. Niestety, powszechność aplikacji internetowych i różnorodność szybko zmieniających się technologii, w których są wytwarzane, sprawiła, iż stały się one częstym celem ataków cybernetycznych. Dodatkowo, w związku z dużym naciskiem na skracanie czasu wytworzenia tego typu rozwiązań informatycznych, coraz częściej systemy oddawane do tzw. produkcyjnego działania posiadają istotne błędy, szczególnie w zakresie bezpieczeństwa [1], [4], [5], [7]. Wiele podatności systemów jest efektem pospiesznego wytwarzania kodu, braku wiedzy i konsultacji z osobami zajmującymi się bezpieczeństwem systemów oraz zaniechania przeprowadzania testów akceptacyjnych w tym zakresie.

Dodatkowo popularność aplikacji internetowych przekłada się na nieustające zainteresowanie nimi hakerów, co sprzyja pojawianiu się coraz to nowszych typów ataków (zagrożeń). W związku z tym, bardzo istotne jest opracowanie skutecznych metodyk szkoleniowych i samych szkoleń z zakresu bezpieczeństwa aplikacji internetowych, które nauczą, w jaki sposób je zabezpieczać i chronić w trakcie już trwającego ataku.

Poziom bezpieczeństwa aplikacji internetowych uzależniony jest w znacznym stopniu od poprawnej implementacji tych aplikacji, a także od wdrożonego systemu zabezpieczeń, chroniącego je przed atakami z cyberprzestrzeni.

Niniejszy artykuł prezentuje propozycję metodyki przeprowadzania szkoleń z zakresu ochrony aplikacji internetowych przed atakami z cyberprzestrzeni. Istotne jest to, iż jednym z elementów metodyki jest środowisko teleinformatyczne wyposażone w różnego typu rozwiązania ochrony aplikacji internetowych, w tym filtry aplikacyjne opracowane przez firmę F5 Networks. Firma specjalizuje się przede wszystkim w opracowywaniu nowych technologii i implementowaniu ich w autorskich produktach, które wdrożone do istniejących sieci teleinformatycznych usprawniają ich działanie oraz wpływają na zwiększenie dostępności i poziomu bezpieczeństwa aplikacji uruchomionych w ramach tych sieci. Omawiany producent systemów zabezpieczeń jest niekwestionowanym liderem, od co najmniej 3 lat, w zestawieniach „Magic Quadrant for Application Delivery Controllers”[1] opracowanych przez firmę Gartner. Warto w tym miejscu podkreślić, że firma F5 Networks prowadzi aktywną współpracę z innymi wiodącymi na rynku producentami rozwiązań informatycznych, takimi jak Microsoft, Cisco, Oracle czy IBM, jak również ze środowiskami akademickimi, czego przykładem jest Wydział Cybernetyki Wojskowej Akademii Technicznej. Współpraca daje Akademii dostęp do najnowszych rozwiązań z zakresu zarządzania ruchem sieciowym, czy też ochrony systemów informatycznych w zakresie zagrożeń występujących w warstwie 7 modelu ISO/OSI, tzw. warstwie aplikacyjnej. Umożliwia to wykorzystanie rozwiązań oferowanych przez F5 Networks w realizacji projektów naukowo-badawczych, prac dyplomowych oraz zajęć edukacyjnych zarówno programowych, jak i w ramach kół zainteresowań, co spotyka się z dużym zainteresowaniem studentów.

Różnorodność produktów oferowanych przez firmę F5 Networks pozwala na opracowanie skutecznego systemu zabezpieczeń i wdrożenie go w istniejącej infrastrukturze sieciowej, w zależności od potrzeb indywidualnych użytkownika, wykorzystując w tym celu jedno rozwiązanie lub wiele rozwiązań połączonych w jeden system bezpieczeństwa. W ofercie firmy F5 Networks można wyróżnić

[1] Ostatni raport „Magic Quadrant for Application Delivery Controllers” został opracowany w 2016 roku.

wiele modułów, różniących się od siebie m.in. przeznaczeniem i funkcjonalnością [13]. Z punktu widzenia kwestii bezpieczeństwa szczególnie interesujący jest BIG-IP Local Traffic Manager (LTM) [8] – rozwiązanie poprawiające dostępność, bezpieczeństwo oraz wydajność aplikacji internetowych, które są coraz częściej krytycznymi z punktu widzenia biznesu. Charakterystyczną cechą tego produktu jest zasada działania w trybie proxy, który pozwala na filtrowanie ruchu sieciowego przesyłanego między klientem a zabezpieczonym serwerem aplikacyjnym. Omawiany produkt firmy F5 dostępny jest w sprzedaży w wielu wersjach fizycznych urządzenia (tzw. appliance) oraz jako system wirtualny. Choć podstawową funkcją omawianego rozwiązania jest zarządzanie ruchem sieciowym, w szczególności możliwość dynamicznego równoważenia obciążenia sieciowego (ang. Load Balancing), to jednak już w standardowym (domyślnym) ukompletowaniu licencyjnym daje ono szeroki wachlarz mechanizmów związanych z bezpieczeństwem, np. funkcje filtrowania transmisji na podstawie informacji zapisywanych w nagłówkach pakietów i segmentów. Należy podkreślić, że możliwości BIG-IP LTM w zakresie ochrony aplikacji internetowych znacząco rozwija opcjonalny moduł o nazwie Application Security Manager (ASM). Jest to moduł umożliwiający ochronę przed zagrożeniami występującymi w warstwie aplikacyjnej (tzw. Web Application Firewall (WAF)), między innymi wymienionymi w zestawieniu OWASP Top 10 [15]: przepełnieniem bufora[2], czy też zatruwaniem plików cookie[3].

Co bardzo istotne, w omawianym produkcie zdefiniowano dużo standardowych zasad bezpieczeństwa, dostosowanych do ochrony wielu popularnych aplikacji webowych, co przyspiesza i ułatwia proces wdrożenia systemu zabezpieczeń. W przypadku wykrycia prób przeprowadzenia ataku na aplikację webową, omawiane rozwiązanie umożliwia przerwanie wykonywania żądania użytkownika, wyświetlenie w oknie jego przeglądarki internetowej stosownego komunikatu o błędzie, a także blokadę podejrzanego ruchu sieciowego nim dotrze on do atakowanej aplikacji webowej.

Wśród cech charakterystycznych BIG-IP LTM firmy F5 należy wskazać autorskie rozwiązanie o nazwie iRule. Bazuje ono na języku skryptowym, który zapewnia bezpośrednią kontrolę przesyłanego ruchu sieciowego pomiędzy klientem a serwerem aplikacyjnym. Za pomocą opracowanych skryptów można

[2] Przepełnienie bufora – atak polegający na wprowadzeniu zbyt dużej ilości danych do bufora aplikacji, co może doprowadzić do sytuacji, w której część przetwarzanych danych zostanie utracona przez błędne działanie aplikacji.

[3] Zatruwanie plików cookie – atak, w ramach którego plik cookie jest modyfikowany przez napastnika celem uzyskania nieautoryzowanego dostępu do serwisu na prawach użytkownika, który jest ofiarą przeprowadzanego ataku.

wykryć ruch sieciowy o sprecyzowanych parametrach, a następnie podjąć stosowną akcję, polegającą na przekierowaniu tego ruchu lub całkowitym jego zablokowaniu, w przypadku gdy wspomniany ruch jest niepożądany z punktu widzenia bezpieczeństwa teleinformatycznego. Użycie omawianego języka skryptowego umożliwia więc precyzyjne dostosowanie systemu zabezpieczeń opartego o rozwiązania firmy F5 Networks w ramach produktu BIG-IP LTM.

Poprawę poziomu bezpieczeństwa, poprzez analizę występujących zagrożeń, a następnie dostosowywania konfiguracji wdrożonego systemu, zapewnia również wbudowany w BIG-IP LTM system raportowania oraz składowania logów. Jest to element pozwalający administratorowi systemu na zachowanie pełnej kontroli nad ruchem sieciowym przesyłanym między użytkownikami a serwerami aplikacyjnymi i dokładną analizę tego ruchu. Wśród zdarzeń rejestrowanych w logu znajdują się zarówno zdarzenia systemowe związane z działaniem (np. uruchomieniem bądź zatrzymaniem) wykorzystywanych modułów, jak i zdarzenia naruszające bezpieczeństwo chronionych aplikacji czy przetwarzanych przez te aplikacje zasobów.

2. Założenia dla metodyki szkoleń w zakresie obrony aplikacji internetowych przed atakami z cyberprzestrzeni

Istotnym czynnikiem warunkującym skuteczność procesu edukacji z zakresu obrony aplikacji internetowych przed atakami z cyberprzestrzeni jest opracowanie odpowiedniej metodyki szkoleń, zgodnie z którą taki proces może zostać przeprowadzony. Należy w tym miejscu podkreślić, że wskazana metodyka powinna zostać przygotowana w taki sposób, aby możliwe było jej wykorzystanie z użyciem określonych narzędzi.

W ramach proponowanej metodyki, za niezbędne należy uznać wskazanie planu ramowego, który w sposób dokładny i czytelny określi przebieg poszczególnych etapów każdego ze spotkań w ramach prowadzonego szkolenia, a ponadto zapewni jego usystematyzowanie [2], [6], [7], [10], [14]. Omawiane działanie jest szczególnie istotne z punktu widzenia dydaktyki, ze względu na potrzebę określenia założeń, które powinny zostać zrealizowane, aby móc uznać przeprowadzone ćwiczenia za skuteczne. Wśród nich wyróżnić można m.in. precyzyjną analizę celu, który powinien być osiągnięty zarówno przez osobę prowadzącą, jak i uczestników. Należy podkreślić, jak ważne z punktu widzenia uczestników szkolenia z zakresu bezpieczeństwa aplikacji internetowych są ćwiczenia praktyczne. Wykorzystanie posiadanej wiedzy w praktyce umożliwia dokładne zrozumienie poruszanego w ramach zajęć problemu oraz poznanie metod, które można wykorzystać w taki sposób, aby określony problem rozwiązać.

Przeznaczenie szkolenia – grupa docelowa

Z potrzeby przekazania szerokiego, ale z drugiej strony już ukierunkowanego i na odpowiednim poziomie zaawansowania, zakresu wiedzy, która jest niezbędna w przypadku rozwiązywania problemów związanych z ochroną aplikacji internetowych przed zagrożeniami z cyberprzestrzeni, wynika konieczność określenia grupy docelowej osób szkolonych. Bazując na praktycznym doświadczeniu, przyjęto, że szkoleniem o wskazanej tematyce powinna być objęta grupa docelowa licząca maksymalnie 20 osób przypadających na jednego instruktora. Grupa ta powinna zostać podzielona na równe, np. 4- lub 5-osobowe podgrupy, co bezpośrednio przekłada się na liczbę potrzebnych stanowisk laboratoryjnych. Im więcej stanowisk laboratoryjnych, tym większe będzie wymagane zaangażowanie ze strony instruktora. Praktyka pokazuje, że przy tego typu złożonych scenariuszach laboratoryjnych na jednego instruktora powinno przypadać nie więcej niż 5 podgrup szkoleniowych. Taki podział jest kluczowy z punktu widzenia efektywności dydaktyki, ponieważ umożliwia osobie prowadzącej szkolenie regularną weryfikację postępu prac w każdej z podgrup, a także pozwala na bieżąco udzielać ewentualnych wskazówek uczestnikom szkolenia, w przypadku wystąpienia u nich problemów lub wątpliwości w trakcie realizacji przydzielonych zadań. Omawianą grupę uczestników stanowić powinni studenci co najmniej III roku studiów technicznych kierunku „informatyka", którzy dokonali wyboru specjalizacji dotyczącej m.in. zagadnień związanych z bezpieczeństwem w sieciach teleinformatycznych.

Cel szkolenia

Zgodnie z przyjętym założeniem, iż ważne jest jasne określenie celu szkolenia, przyjęto, że szkolenie powinno zapewnić:

- poznanie przez uczestników szkolenia istoty zagrożeń (być może tylko wybranych powiązanych z danym szkoleniem), na które mogą być narażone aplikacje internetowe,
- osiągnięcie określonego poziomu umiejętności badania tych aplikacji np. za pomocą skanerów bezpieczeństwa, w celu wykrycia ich podatności na ataki z cyberprzestrzeni,
- rozwój umiejętności precyzyjnego definiowania źródła (przyczyn) wykrytych podatności, np. wskutek niepoprawnej konfiguracji badanej aplikacji internetowej,

- rozwój umiejętności rozwiązywania problemu związanego z bezpieczeństwem badanej aplikacji internetowej z wykorzystaniem dostępnych narzędzi i urządzeń teleinformatycznych,
- rozwój umiejętności testowania skuteczności wdrożonego systemu ochrony aplikacji internetowej,
- rozwój umiejętności prezentowania wyników swojej pracy przez uczestników szkolenia.

Przebieg szkolenia

W świetle prowadzonych rozważań związanych z opracowaniem skutecznej metodyki przeprowadzania szkoleń z zakresu ochrony aplikacji internetowej przed zagrożeniami z cyberprzestrzeni ustalono plan ramowy, zgodnie z którym powinien być realizowany program szkoleniowy. Składa się on ze zbioru najważniejszych, kolejno następujących po sobie etapów, a mianowicie:

1. Opracowania scenariusza zajęć przed rozpoczęciem spotkania szkoleniowego.
2. Przedstawienia uczestnikom tematu poruszanego w ramach spotkania szkoleniowego oraz celu jego realizacji.
3. Weryfikacji wiedzy, z zakresu którego dotyczy spotkanie szkoleniowe, posiadanej przez uczestników.
4. Wprowadzenia teoretycznego do problemu, stanowiącego podstawę zadań przedstawionych w scenariuszu szkoleniowym realizowanych przez uczestników.
5. Omówienia punktów kontrolnych, które będą podlegały ocenie w trakcie prowadzonych zajęć szkoleniowych.
6. Etapu realizacji zadań przydzielonych uczestnikom w trakcie spotkania szkoleniowego.
7. Oceny wyników pracy uzyskanych podczas prowadzonych zajęć przez uczestników szkolenia.
8. Opracowania sprawozdania z przebiegu zajęć szkoleniowych, zawierającego wyniki pracy poszczególnych uczestników oraz wnioski wyciągnięte z rozwiązywanych przez nich problemów.
9. Końcowej oceny uczestnika szkolenia na podstawie zrealizowanych przez niego zadań.

Warto zauważyć, że przedstawienie planu ramowego szkolenia umożliwia

w sposób poglądowy zapoznanie się z jego przebiegiem oraz strukturą tematyczną. Na potrzeby niniejszego celu należy uznać za zasadne precyzyjne zdefiniowanie każdego z wymienionych etapów spotkania szkoleniowego.

Pierwszym z omawianych etapów, przedstawionym w ramach metodyki szkoleniowej, jest etap związany z opracowaniem scenariusza szkoleniowego, który stanowi istotny element prowadzonych zajęć. Scenariusz ten może zostać przekazany uczestnikom szkolenia w postaci instrukcji, zawierającej dużo informacji i zagadnień dotyczących realizowanego w ramach spotkania tematu. Wśród informacji w nim zawartych należy wyróżnić m.in.:

1. Określenie tematu zajęć spotkania szkoleniowego.
2. Wykaz umiejętności, które powinien zdobyć uczestnik szkolenia w wyniku realizacji zadań przydzielonych do wykonania w trakcie zajęć szkoleniowych, np.:
   - badanie podatności aplikacji internetowych na ataki z cyberprzestrzeni,
   - znajomość metod ochrony aplikacji internetowej przed zagrożeniami typu *SQL Injection*, *XSS* itp.,
   - umiejętność wdrożenia podstawowego systemu ochrony dla aplikacji internetowej,
   - rozpoznawanie symptomów ataku na aplikację internetową na podstawie dziennika zdarzeń systemu ochrony takiej aplikacji.
3. Chronologiczny wykaz zadań, które powinny zostać zrealizowane przez uczestnika szkolenia. Jeśli określone zadanie tego wymaga, niezbędne jest wskazanie stosownych parametrów konfiguracyjnych, które zostaną wykorzystane w trakcie rozwiązywania zadania. Takie parametry mogą stanowić np. wykorzystywana adresacja IP urządzeń lub maszyn wirtualnych, dane uwierzytelniające użytkowników itp.
4. Wykaz pytań kontrolnych wynikających z przebiegu realizacji przedstawionych zadań, na które uczestnik powinien udzielić odpowiedzi pisemnej lub ustnej w trakcie prezentacji wyników swojej pracy.
5. Wykaz zaleceń i wymagań dotyczących opracowania przez uczestnika sprawozdania z realizacji zadań, otrzymanych w ramach zajęć szkoleniowych.

Opracowanie scenariuszy szkoleniowych ma na celu usystematyzowanie zagadnień, które stanowią temat zajęć szkoleniowych i umożliwienie precyzyjnego określenia wymagań dotyczących realizacji zadań przez uczestników takiego szkolenia.

Kolejny z omawianych etapów przebiegu spotkania szkoleniowego jest ściśle związany z prezentacją uczestnikom tematu zajęć, którego strukturę tworzą odpowiednio dobrane zagadnienia. Należy w tym miejscu nadmienić, że omawiany punkt jest istotny z punktu widzenia dydaktycznego, zważywszy na możliwość zaprezentowania genezy poruszanego problemu, a tym samym potrzebę zwrócenia uwagi słuchaczy na jego znaczenie w kwestii zapewnienia bezpieczeństwa aplikacjom internetowym. Etap ten pozwala także wstępnie ukierunkować pogląd na omawiany problem, w celu późniejszej jego analizy oraz dążenia do uzyskania rozwiązania w możliwie dokładny i precyzyjny sposób. Należy zaznaczyć, że skuteczna realizacja tego celu zależy od wykorzystania takich instrumentów, jak: własna wiedza uczestnika, materiały naukowe w formie elektronicznej, dostępne oprogramowanie oraz rozwiązania fizyczne w postaci urządzeń teleinformatycznych.

Trzeci punkt przedstawionego planu ramowego szkolenia z zakresu ochrony aplikacji internetowych dotyczy weryfikacji wiedzy posiadanej przez uczestników danego szkolenia. Weryfikacja ta ma na celu określenie poziomu zaawansowania uczestników we wspomnianym zakresie np. poprzez wymianę poglądów i informacji na temat zagadnień, których dotyczy spotkanie szkoleniowe, w formie dialogu pomiędzy osobą prowadzącą a uczestnikami. Przedmiotowa rozmowa umożliwia dostosowanie sposobu przekazywania wiedzy przez osobę prowadzącą w dalszych etapach szkolenia, tak aby prezentowane informacje były w pełni zrozumiane przez odbiorców, a także umożliwiły im dobre przyswojenie wiedzy związanej z zadaniami, które będą realizowane w trakcie trwania szkolenia. Warto podkreślić, że uczestnicy szkolenia w trakcie omawianego etapu nie powinni podlegać ocenie przez osobę prowadzącą, co pozwoli uzyskać większą swobodę wypowiedzi uczestników szkolenia oraz ich większe zaangażowanie i chęć zrozumienia poruszanego problemu. Ewentualną formę oceny na tym etapie może stanowić wyróżnienie ponadprzeciętnej aktywności uczestnika szkolenia, która zostanie uwzględniona w momencie podsumowania jego osiągnięć dokonanych w trakcie całego spotkania szkoleniowego.

Charakteryzując metodykę przeprowadzania szkoleń, należy zdefiniować kolejny z etapów, który stanowi wprowadzenie teoretyczne do rozwiązywanego problemu. Jest to również istotny etap zajęć szkoleniowych ze względu na możliwość szczegółowego przedstawienia słuchaczom problemu wraz z czynnikami, które mu towarzyszą. Biorąc pod uwagę zakres tematyki, której dotyczy omawiana metodyka szkolenia, należy wskazać, że na tym etapie osoba prowadząca posiada m.in. możliwość scharakteryzowania zagrożeń, na które podatne mogą być badane aplikacje internetowe oraz skupienie szczególnej uwagi na zagrożeniach, które mogą wystąpić w trakcie realizacji zadań przez osoby uczestniczące w szkoleniu. Ze względu na charakter omawianego etapu,

należy także wspomnieć, że umożliwia on słuchaczom dokładne zrozumienie istoty problemu związanego z bezpieczeństwem aplikacji internetowych, zaś w przypadku wystąpienia u uczestników jakichkolwiek wątpliwości, czy potrzeby uzyskania dodatkowych informacji związanych z tematem zajęć, mogą one być przedstawione osobie prowadzącej, co gwarantuje możliwość uzyskania na nie odpowiedzi, jak również wskazania dostępnych materiałów źródłowych.

W ramach etapu piątego omawianej metodyki szkolenia należy podkreślić wymóg precyzyjnego określenia punktów kontrolnych podlegających częściowej ocenie. Punkty kontrolne mogą stanowić wybrane zadania, które powinien zrealizować uczestnik szkolenia w trakcie trwania zajęć szkoleniowych, a następnie po ich wykonaniu jest on zobowiązany do przedstawienia postępu prac osobie prowadzącej. Takie postępowanie ma na celu weryfikację stopnia realizacji przydzielonych zadań, sposobu ich wykonania przez uczestnika szkolenia, a tym samym zapewnienia dalszej realizacji pracy. Należy także podkreślić, że wskazanie punktów kontrolnych oraz poinformowanie o wyborze tych punktów uczestników szkolenia jest istotne z punktu widzenia oceniania wyników pracy poszczególnych osób. Punkty te mogą stanowić podstawę oceny uczestnika szkolenia, w przypadku gdy dany uczestnik nie jest w stanie w pełni zrealizować przydzielonych mu zadań w trakcie trwania spotkania szkoleniowego. Co bardzo ważne, punkty te powinny zostać wyznaczone w sposób proporcjonalny do stopnia trudności wykonywanego zadania oraz czasu, który jest wymagany do jego wykonania. Za konieczne należy również uznać przydzielenie oceny punktowej lub procentowej każdemu z punktów kontrolnych, tak aby osoba prowadząca miała stosowne podstawy do oceny uczestnika realizującego otrzymane zadania.

Kolejny prezentowany etap metodyki jest etapem głównym zajęć szkoleniowych. W jego zakresie uczestnicy powinni zrealizować zadania otrzymane od osoby prowadzącej. Przed przystąpieniem do wykonywania pracy konieczne jest określenie punktu startowego, niezbędnego do poprawnego przebiegu zajęć szkoleniowych. W punkcie tym uczestnik powinien zweryfikować poprawność podstawowej konfiguracji wykorzystywanego środowiska, np. poprzez sprawdzenie wzajemnej osiągalności wykorzystywanych maszyn wirtualnych lub urządzeń sieciowych, ich dostępności oraz poprawnego działania. Jest to warunek konieczny do zrealizowania, ponieważ jego poprawność determinuje możliwość dalszego wykonywania prac w ramach udziału w zajęciach szkoleniowych. W przypadku wystąpienia problemów związanych z konfiguracją środowiska, uniemożliwiających wykonywanie zadań, fakt ten należy niezwłocznie zgłosić osobie prowadzącej szkolenie. Jeśli środowisko pracy działa w sposób poprawny, to uczestnik powinien przystąpić do wykonywania zadań zgodnie z otrzymanym scenariuszem szkoleniowym, przedstawiając postęp prac w odniesieniu do wyznaczonych punktów kontrolnych. Co bardzo istotne,

przebieg omawianego etapu zależy przede wszystkim od opracowanego scenariusza szkolenia i może być realizowany w następujący sposób:

1. Weryfikacja poprawności konfiguracji wykorzystywanego środowiska.
2. Badanie podatności aplikacji internetowej na zagrożenia z cyberprzestrzeni z wykorzystaniem skanerów bezpieczeństwa.
3. Przeprowadzenie próby ataku na niezabezpieczoną aplikację internetową, na podstawie informacji przedstawionych w raportach skanerów bezpieczeństwa.
4. Wdrożenie systemu ochrony aplikacji internetowej z wykorzystaniem dodatkowego oprogramowania lub urządzenia fizycznego.
5. Dostosowanie konfiguracji wdrożonego systemu ochrony aplikacji internetowej.
6. Ponowne badanie podatności aplikacji internetowej na ataki z cyberprzestrzeni.

Bardzo ważnym czynnikiem mającym wpływ na efektywność szkolenia jest, by jego uczestnik na każdym etapie prac miał zapewnioną możliwość dokumentowania ich przebiegu, np. na podstawie zrzutów ekranu przedstawiających:

- wykryte podatności badanej aplikacji internetowej,
- skuteczne wykonanie ataku na badaną aplikację webową,
- konfigurację wdrożonego systemu ochrony aplikacji webowej,
- skuteczność wdrożonego systemu ochrony aplikacji webowej poprzez zablokowanie próby ataku.

Wyniki uzyskane w trakcie trwania tego etapu stanowią podstawę oceny uczestnika przez osobę prowadzącą.

Punkt siódmy omawianej metodyki szkoleń stanowi ocena pracy uczestnika szkolenia, którą dany uczestnik wykonał w trakcie trwania zajęć. Na tym etapie istnieje możliwość określenia przez osobę prowadzącą tego, czy dany uczestnik wykonał zadanie poprawnie, czy zostało ono wykonane w pełni, czy wyłącznie do określonego momentu. Ocena osiągnięć uczestnika jest wyznaczana na podstawie uprzednio zweryfikowanych postępów pracy w punktach kontrolnych, a także na podstawie prezentacji środowiska w trakcie trwania niniejszego etapu. Wyznaczenie stosownej oceny za realizację zadania jest możliwe np. na podstawie zdobytych punktów lub procentowego stopnia wykonania przydzielonych uczestnikowi zadań. Warto także wspomnieć, że w ocenie pracy w trakcie zajęć szkoleniowych należy uwzględnić ponadprzeciętną aktywność uczestników szkolenia w trakcie etapu trzeciego, jeżeli taka sytuacja miała miejsce.

Kolejnym etapem przedstawianej metodyki przeprowadzania szkoleń z zakresu ochrony aplikacji internetowej przed atakami z cyberprzestrzeni jest opracowanie przez uczestnika takiego szkolenia sprawozdania z realizacji otrzymanych zadań. W dokumencie sprawozdania powinny zostać umieszczone wymagane informacje, które zostały określone w scenariuszu szkoleniowym. Dokument sprawozdania z wykonania zadań przez uczestnika powinien świadczyć o zrozumieniu przez niego realizowanego tematu, a także zawierać dokumentację wykonanych czynności, które pozwoliły na zrealizowanie zadań. Istotnym wymaganym elementem dokumentu sprawozdania są wnioski uczestnika szkolenia, zawierające własne spostrzeżenia na temat rozwiązywanego problemu w ramach zajęć szkoleniowych, opinie na temat wykorzystywanego oprogramowania bądź urządzenia, a także uwagi dotyczące całego przebiegu zajęć szkoleniowych.

Ostatnim etapem omawianym w ramach opracowanej metodyki szkoleniowej jest końcowa ocena uczestnika danego szkolenia. Na przedmiotową ocenę składa się ocena otrzymana przez uczestnika po realizacji i prezentacji uzyskanych wyników w trakcie zajęć szkoleniowych oraz ocena przydzielona na podstawie opracowanego dokumentu sprawozdania. Warto w tym miejscu zauważyć, że choć dokument sprawozdania jest dokumentem niezbędnym do ocenienia dokonań uczestnika szkolenia, nie stanowi on jednak podstawy oceny, natomiast umożliwia ewentualną poprawę lub obniżenie oceny otrzymanej przez uczestnika szkolenia w trakcie zajęć szkoleniowych. Wydaje się to zasadne z punktu widzenia dydaktycznego, ze względu na ilość pracy, którą uczestnik powinien wykonać w trakcie zajęć szkoleniowych z wykorzystaniem ograniczonej ilości materiałów dodatkowych, w stosunku do pracy poświęconej na wykonanie dokumentu sprawozdania po zajęciach szkoleniowych.

Przedstawiona w ramach niniejszego rozdziału metodyka przeprowadzania szkoleń jest ściśle związana z odpowiednio przygotowanym stanowiskiem laboratoryjnym. W związku z tym, za stosowne należy uznać przedstawienie projektu takiego stanowiska.

Stanowisko laboratoryjne

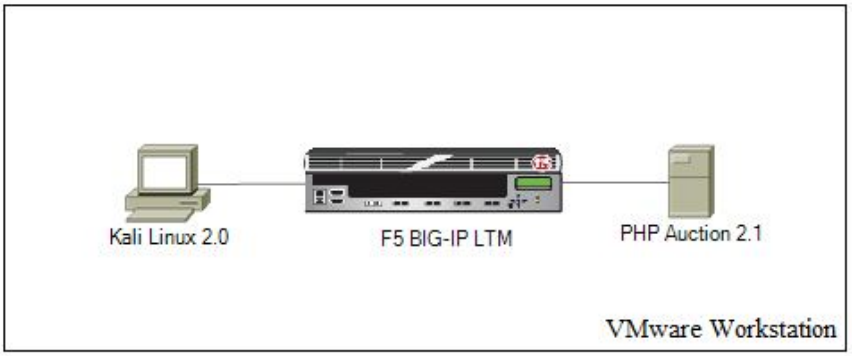
Przyjęto, że omawiane stanowisko laboratoryjne opracowane zostanie w postaci w pełni zwirtualizowanej, tzn. że zbudowana infrastruktura teleinformatyczna będzie stanowić odwzorowanie rzeczywistej topologii przy użyciu maszyn wirtualnych. Należy przy tym wskazać, że uwzględniono również możliwość odwzorowania stanowiska z wykorzystaniem urządzeń

w wersji fizycznej. W ramach stanowiska wykorzystano następujące rozwiązania:

- wersja zwirtualizowana produktu BIG-IP LTM (z licencją dla modułu ASM) lub jego wersja fizyczna,
- maszyna wirtualna z zainstalowanym systemem operacyjnym Kali Linux w wersji 2.0,
- maszyna wirtualna z zainstalowanym systemem Linux, udostępniająca usługę WWW o nazwie PHP Auction w wersji 2.1. Jest to testowy system aukcyjny, który celowo posiada wiele podatności na zagrożenia, w związku z czym może zostać wykorzystany jako obiekt testowy w trakcie realizacji zadań szkoleniowych.

Przedstawione w wykazie rozwiązania umożliwiają przygotowanie wirtualnego środowiska teleinformatycznego zapewniającego filtrowanie w warstwie aplikacji ruchu sieciowego, przesyłanego między klientem a podatnym na ataki serwerem aplikacyjnym.

Poglądową topologię, która zostanie utworzona w ramach implementacji projektu z wykorzystaniem omówionych maszyn wirtualnych, przedstawiono na rysunku 1.



Rys. 1. Topologia zwirtualizowanego stanowiska szkoleniowego

Bazując na opracowanej metodyce szkoleniowej, zbiorze produktów, które mogą zostać wykorzystane oraz przeznaczeniu dydaktycznym opracowywanego stanowiska laboratoryjnego, wyodrębnione zostały następujące wymagania funkcjonalne z nim związane:

- wykorzystanie jak najmniejszej liczby urządzeń fizycznych oraz maszyn wirtualnych,
- możliwość badania aplikacji webowej pod kątem znanych podatności, przede wszystkim na ataki wywodzące się z grup zagrożeń *Injection*, *Cross-Site Scripting* oraz *Sensitive Data Exposure*,

- możliwość przeprowadzenia kontrolowanych ataków na badaną aplikację webową,
- możliwość uruchomienia systemu ochrony badanej aplikacji, w celu zabezpieczenia występujących podatności, które zostały w niej wykryte.

Przykładowe szkolenie

Prezentowane przykładowe szkolenie powinno trwać 8 godzin i jest podzielone na 2 scenariusze. Należy podkreślić, że niezbędne jest poprawne zrealizowanie przez uczestnika zadań określonych w scenariuszu pierwszym, z uwagi na to, że zadania zawarte w scenariuszu drugim stanowią rozwinięcie i kontynuację wykonanych w ramach pierwszego spotkania etapów konfiguracyjnych.

W ramach spotkań szkoleniowych uwzględniono kwestie przygotowania infrastruktury teleinformatycznej zbudowanej z wykorzystaniem trzech maszyn wirtualnych, ich wstępnej konfiguracji, przeprowadzenia badań związanych z atakami typu *DoS*, *Injection* oraz *Cross-Site Scripting*, a także wdrożenia systemu ochrony aplikacji internetowej w postaci rozwiązania BIG-IP LTM z aktywnym modułem ASM (w skrócie dalej BIG-IP LTM/ASM) firmy F5 Networks oraz badania skuteczności wdrożonego systemu.

Scenariusz 1. Uruchomienie środowiska laboratoryjnego, wstępna konfiguracja produktu BIG-IP LTM z aktywnym modułem ASM, ochrona aplikacji webowej przed atakiem typu *DoS*.

Czas trwania: 4 godziny

Cel zajęć: Nauczenie podstaw konfiguracji rozwiązania BIG-IP LTM/ASM, wykrywania podatności aplikacji webowej i jej ochrony przed zagrożeniami typu *DoS*.

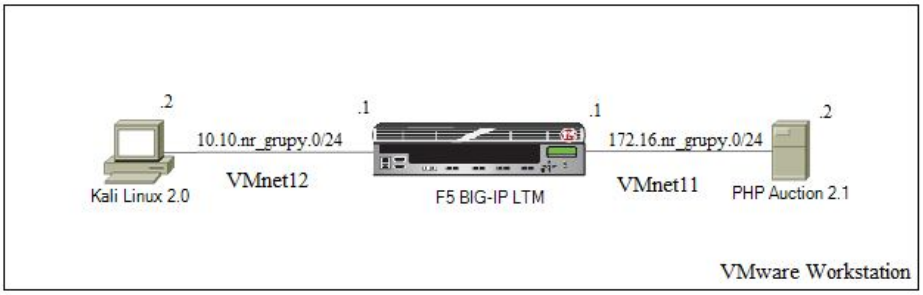
Zakres realizowanych zadań (etapy):

1. uruchomienie środowiska wirtualnego z wykorzystaniem oprogramowania VMware Workstation, w tym wstępne skonfigurowanie rozwiązania BIG-IP LTM/ASM,
2. badanie podatności aplikacji webowej na ataki typu *DoS*,
3. wdrożenie systemu ochrony aplikacji webowej z wykorzystaniem BIG-IP LTM/ASM oraz badanie jego skuteczności.

W trakcie realizacji przedstawionych zadań zaleca się jednoczesną dokumentację osiąganych wyników zgodnie z punktem „Sprawozdanie”.

Etap 1 – uruchomienie środowiska wirtualnego

Celem etapu 1 jest konfiguracja środowiska laboratoryjnego[4], którego schemat przedstawiono na rys. 2. Po zakończeniu tej konfiguracji należy sprawdzić wzajemną osiągalność maszyn wirtualnych, a uzyskany wynik pracy przedstawić osobie prowadzącej. Czas realizacji tego etapu jest oszacowany na ok. 2 godziny.



Rys. 2. Topologia wirtualna rozszerzona o maszynę BIG-IP

Elementem zasługującym na szczególną uwagę w realizacji etapu 1, z racji tematu tego artykułu, jest kwestia wstępnej konfiguracji rozwiązania BIG-IP LTM/ASM. Na początku szkolenia będzie ono pracowało w trybie monitoringu, czyli przekazywało ruch sieciowy bez podejmowania względem niego jakiejkolwiek akcji. Maszyna wirtualna dla BIG-IP LTM/ASM wymaga uruchomienia trzech interfejsów sieciowych: dwóch dla obsługi ruchu przekazywanego pomiędzy systemami Kali i PHP Auction, zaś trzeciego do zarządzania BIG-IP LTM/ASM. Po uruchomieniu maszyny F5 BIG-IP należy zalogować się do systemu (dane uwierzytelniające – login: *root*, hasło: *default*), a następnie skonfigurować interfejs zarządzający (polecenie *config*)[5] i sprawdzić osiągalność sieci Internet (np. ping 8.8.8.8)[6]. Jeśli wszystko działa prawidłowo, należy z komputera hosta nawiązać połączenie z adresem interfejsu zarządzającego maszyny BIG-IP LTM/ASM za pomocą przeglądarki internetowej (*https://adres_interfejsu_zarządzającego*) i zalogować się do maszyny BIG-IP – login: *admin*, hasło: *admin*. Kolejnym krokiem jest

[4] Pełna instrukcja laboratoryjna zawiera również szczegółowe opisy konfiguracji połączeń pomiędzy wirtualnymi maszynami (wykorzystane interfejsy wirtualne, tryby ich pracy itd.). Ustawienie adresów IP przed uruchomieniem wirtualnych maszyn jest wymagane ze względu na równoczesną pracę kilku podgrup szkoleniowych – zakłada się, że każda podgrupa działa w odmiennym zakresie adresowym, co zabezpiecza przed ewentualnymi konfliktami adresów IP.

[5] Na urządzeniach fizycznych adres IP interfejsu zarządzającego ustawia się z wykorzystaniem przycisków umieszczonych na przednim panelu urządzenia.

[6] Połączenie z Internetem jest konieczne do zainstalowania licencji dla BIG-IP LTM/ASM.

wprowadzenie numeru licencji uzyskanego od osoby prowadzącej, a następnie aktywowanie produktu BIG-IP LTM/ASM. Potem należy sprawdzić, czy został prawidłowo aktywowany moduł *Application Security Manager* (ASM) i poczekać na uaktualnienie konfiguracji maszyny BIG-IP LTM/ASM. Dalsza konfiguracja BIG-IP LTM/ASM w zakresie samego przekazywania ruchu pomiędzy systemami Kali i PHP Auction wymaga:

1. skonfigurowania dwóch sieci VLAN (*Internal* dla ruchu lokalnego między serwerem aplikacyjnym a rozwiązaniem BIG-IP, *External* dla ruchu pomiędzy systemem Kali Linux a systemem BIG-IP). Należy do nich przypisać odpowiednie interfejsy sieciowe maszyny wirtualnej BIG-IP,
2. przypisania adresów IP interfejsom maszyny BIG-IP LTM/ASM, przydzielonym do poszczególnych sieci VLAN (zgodnie z rys. 2),
3. dokonania weryfikacji wzajemnej osiągalności wykorzystywanych maszyn wirtualnych (uzyskany wynik pracy należy przedstawić osobie prowadzącej),
4. utworzenia serwera wirtualnego (adres docelowy serwera: *10.10.nr_grupy.1:80*), z ustawionym profilem na wartość *HTTP* oraz uruchomioną translacją adresów sieciowych (tryb *Auto Map*[7]).
5. zdefiniowania nowej puli adresowej (*Default Pool*), w której należy wskazać adres sieciowy serwera aplikacji webowej (PHP Auction). Po odczekaniu ok. 1 minuty należy zweryfikować status zdefiniowanego serwera wirtualnego,
6. zweryfikowania osiągalności zdefiniowanego serwera wirtualnego z maszyny Kali Linux (uzyskany wynik pracy należy przedstawić osobie prowadzącej).

Zakończenie z powodzeniem ww. etapów konfiguracyjnych świadczy o odpowiednim przygotowaniu stanowiska laboratoryjnego i tym samym o możliwości rozpoczęcia zadań będących zasadniczym celem szkolenia.

Etap 2 – badanie podatności aplikacji webowej na ataki typu *DoS*

W celu realizacji tego etapu należy:

1. w systemie Kali Linux uruchomić sniffer Wireshark, a następnie przeprowadzić próbę ataku DoS na serwer aplikacyjny za pomocą programu GoldenEye. W trakcie ataku obserwować dostępność strony aukcyjnej PHP Auction za pomocą przeglądarki WWW,

[7] Tryb translacji *Auto Map* – tryb ten umożliwia translację adresów sieciowych w oparciu o jeden ze zdefiniowanych uprzednio adresów IP przypisanych do istniejących interfejsów maszyny BIG-IP.

2. odpowiedzieć na następujące pytania:
   a. Czy w trakcie ataku strona aukcyjna była dostępna?
   b. Jakie objawy występowały w trakcie trwania ataku?
   c. Jakiego rodzaju pakiety przesyłane są w trakcie trwania ataku?
   d. Jaka jest częstotliwość przesyłanych pakietów?

Czas realizacji tego etapu jest oszacowany na ok. 30 minut.

Etap 3 – wdrożenie systemu ochrony aplikacji webowej z wykorzystaniem BIG-IP LTM/ASM oraz badanie jego skuteczności

W celu realizacji tego etapu należy:

1. zdefiniować nowy profil ochrony aplikacji webowej przed atakami *DoS*. Dokonać konfiguracji profilu z wykorzystaniem wartości parametru *TPS* (liczba nowych połączeń na sekundę z jednego adresu sieciowego), dobierając parametry stosownie do wydajności sprzętu komputerowego, na którym realizowane jest zadanie,
2. utworzony profil przypisać do zdefiniowanego serwera wirtualnego. Przeprowadzić próbę ataku DoS i zweryfikować poprawność konfiguracji systemu ochrony. W przypadku niskiej skuteczności dostosować konfigurację profilu i ponownie przeprowadzić testy (uzyskany wynik pracy przedstawić osobie prowadzącej),
3. odpowiedzieć na następujące pytania:
   a. W jaki sposób system BIG-IP zapobiega atakom DoS?
   b. W jaki sposób można wykazać skuteczność wdrożonego systemu ochrony aplikacji webowej?

Czas realizacji tego etapu jest oszacowany na ok. 1,5 godziny.

W ramach sprawozdania z realizacji otrzymanego zadania szkoleniowego, uczestnik powinien udokumentować poszczególne etapy pracy, w formie zrzutów ekranowych z odpowiednim komentarzem oraz wnioskami:

1. Etap konfiguracji środowiska wirtualnego:
   a. wzajemna osiągalność maszyn wirtualnych (polecenie ping),
   b. dostępność portalu aukcyjnego z poziomu przeglądarki internetowej w trakcie przeprowadzanego ataku DoS,
   c. osiągalność sieci Internet z maszyny wirtualnej BIG-IP,
2. Etap wdrożenia i testowania systemu ochrony BIG-IP LTM/ASM, w opisie którego znajdą się odniesienia do wyników uzyskanych w analogicznych próbach naruszeń wykonanych w etapie 2:

a. konfiguracja VLAN-ów,
b. konfiguracja interfejsów sieciowych,
c. konfiguracja profilu serwera wirtualnego,
d. wzajemna osiągalność maszyn wirtualnych (polecenie ping),
e. konfiguracja profilu ochrony przed atakami typu DoS,
f. okno konsoli w trakcie przeprowadzania ataku DoS,
g. dostępność aplikacji webowej w trakcie przeprowadzania ataku,
h. wykresy w środowisku BIG-IP dotyczące wykrytego ataku DoS.

Uczestnik szkolenia w sprawozdaniu powinien umieścić odpowiedź pisemną na pytania zawarte w niniejszym scenariuszu.

Scenariusz 2. Badanie podatności aplikacji webowej PHP Auction, implementacja systemu ochrony przed atakami z grupy *Injection* oraz *Cross-Site Scripting*.

Czas trwania: 4 godziny

Cel zajęć: Nauczenie sposobów wykrywania i weryfikowania podatności aplikacji webowych z grupy *injection* i *XSS*, a także metod ochrony podatnej aplikacji z wykorzystaniem produktu BIG-IP LTM/ASM.

Zakres realizowanych zadań (etapy):

1. badanie podatności aplikacji webowej na ataki typu *injection* oraz Cross-Site-Scripting,
2. konfiguracja produktu BIG-IP firmy F5 – tworzenie profilu zabezpieczeń, a następnie dostosowywanie zbudowanego profilu,
3. badanie skuteczności wdrożonego systemu ochrony.

W trakcie realizacji przedstawionych zadań zaleca się jednoczesną dokumentację osiąganych wyników zgodnie z punktem „Sprawozdanie”.

Etap 1 – badanie podatności aplikacji webowej na ataki typu *injection* oraz Cross-Site-Scripting

W celu realizacji tego etapu należy:

1. uruchomić wszystkie maszyny w opracowanym środowisku wirtualnym,

2. sprawdzić wzajemną osiągalność maszyn (np. poleceniem ping),
3. wykorzystując skanery podatności aplikacji internetowych (np. Vega, Golismero), zbadać aplikację PHP Auction pod kątem wykrycia luk związanych z atakami *injection* oraz *Cross-Site Scripting*,
4. odpowiedzieć na pytania:
   a. Jakie elementy aplikacji mogą być podatne na przeprowadzenie ataku?
   b. W jaki sposób można przeprowadzić atak, wykorzystując wykryte w trakcie badania podatności?
   c. Jakie konsekwencje mogą wynikać z ataku zakończonego sukcesem?
5. przeprowadzić próby ataku na aplikację webową, wykorzystując wykryte podatności. Wykonać przynajmniej 3 różne skuteczne ataki,
6. wyniki prób zakończonych sukcesem przedstawić osobie prowadzącej wraz z wyjaśnieniem sposobu ataku.

Czas realizacji tego etapu jest oszacowany na ok. 1,5 godziny.

Etap 2 – konfiguracja systemu ochrony aplikacji webowej

W celu realizacji tego etapu należy:

1. zalogować się do panelu administracyjnego maszyny BIG-IP LTM/ASM,
2. utworzyć nowy profil zabezpieczeń, przypisany do zdefiniowanego, w ramach realizacji pierwszego scenariusza serwera wirtualnego (wykorzystać w kreatorze metodę zaawansowaną – „Create a security policy manually or use templates (advanced)"),
3. odpowiedzieć na następujące pytania:
   a. Jakie parametry przekazywane są przez użytkownika do aplikacji PHP Auction? Wymienić co najmniej 5.
   b. W jaki sposób chronić zasoby aplikacji webowej przed atakami związanymi z przekazywanymi parametrami?
   c. W jakim trybie należy uruchomić profil zabezpieczeń? Transparent czy Blocking? Czym różnią się te tryby?
4. zdefiniować listę podstawowych parametrów i przypisać do każdego z nich stosowne sygnatury ataku,
5. dokonać kilku prób ataku na aplikację webową (można w tym celu wykorzystać skaner podatności),

6. zweryfikować proces „uczenia" systemu ochrony (menu Security/Application Security/Policy Building/Manual Traffic Learning). Uzyskane wyniki pracy przedstawić osobie prowadzącej,
7. zweryfikować zawartość przedstawionych kategorii naruszeń bezpieczeństwa, a następnie zatwierdzić lub odrzucić wybrane wpisy,
8. powtarzając kroki z punktów 5-7, uzupełnić konfigurację profilu zabezpieczeń.

Czas realizacji tego etapu jest oszacowany na ok. 2,5 godziny.

Etap 3 – weryfikacja skuteczności skonfigurowanego systemu ochrony

W celu realizacji tego etapu należy:

1. dokonać ponownego badania aplikacji webowej za pomocą skanera podatności (istotne jest, aby użyć takiej samej konfiguracji skanera jak w trakcie realizacji etapu 1, punktu 3). Porównać otrzymane wyniki z wynikami z etapu badania podatności aplikacji,
2. ponownie przeprowadzić próby ataku na aplikację webową. Próby te powinny przebiegać w sposób identyczny, jak w trakcie realizacji punktu 5 etapu 1,
3. skorzystać z dziennika zdarzeń maszyny F5, w celu weryfikacji zapisanych logów (uzyskane wyniki pracy przedstawić osobie prowadzącej).

Czas realizacji tego etapu jest oszacowany na ok. 30 minut.

W ramach sprawozdania z realizacji otrzymanego zadania szkoleniowego, uczestnik powinien udokumentować poszczególne etapy pracy, w formie zrzutów ekranowych z odpowiednim komentarzem oraz wnioskami:

1. Etap badania podatności aplikacji webowej:
   a. raport skanera bezpieczeństwa,
   b. efekty przeprowadzanych ataków na aplikację webową.
2. Etap konfiguracji systemu ochrony aplikacji webowej:
   a. definicja utworzonego profilu zabezpieczeń,
   b. wykaz zdefiniowanego zbioru monitorowanych parametrów,
   c. konfiguracja jednego ze zdefiniowanych parametrów,
   d. wykaz kategorii naruszeń bezpieczeństwa w trakcie procesu „nauczania" systemu ochrony,
   e. zawartość dwóch wybranych kategorii naruszeń bezpieczeństwa w omawianym procesie.

3. Etap weryfikacji skuteczności skonfigurowanego systemu ochrony:
   a. raport skanera bezpieczeństwa,
   b. efekty przeprowadzanych ataków na aplikację webową,
   c. zawartość dziennika zdarzeń systemu BIG-IP LTM/ASM,
   d. widok szczegółów każdego ze zdarzeń, które zostało zapisane w dzienniku, w trakcie przeprowadzania ataków na aplikację webową.

Uczestnik w sprawozdaniu powinien umieścić odpowiedź pisemną na pytania zadane w ramach niniejszego scenariusza.

Oba scenariusze zostały sprawdzone w praktyce, w szczególności w zakresie skuteczności wprowadzonych zabezpieczeń. Szkolenie na początku wykazało podatności ochranianej aplikacji, a następnie sposoby (mechanizmy), które pozwalają zablokować ataki kierowane na – cały czas istniejące w aplikacji – podatności.

3. Podsumowanie

W artykule skupiono się na przedstawieniu założeń dla metodycznego przeprowadzenia szkolenia z zakresu ochrony aplikacji internetowych przed atakami z cyberprzestrzeni. Opisano metodykę prowadzenia tego typu szkoleń, jak również stanowisko laboratoryjne, opracowane specjalnie na potrzeby realizacji części praktycznej wraz z przygotowanymi scenariuszami zadań szkoleniowych. Wydaje się, że stanowi spójną całość i umożliwia przekazywanie wiedzy w sposób usystematyzowany i w pełni zrozumiały przez odbiorców.

W ramach opracowanej metodyki przedstawiono plan ramowy oraz charakterystykę każdego z występujących etapów w trakcie szkolenia. Tak zdefiniowana metodyka umożliwia przeprowadzenie zajęć szkoleniowych w jednolity (powtarzalny) i precyzyjnie określony sposób. Autorzy artykułu mają nadzieję, że rzetelnie przygotowane scenariusze, stanowisko laboratoryjne oraz przemyślana i sprawdzona w praktyce metodyka prowadzenia tego typu szkolenia będą miały znaczące przełożenie na zainteresowanie słuchaczy tematyką bezpieczeństwa aplikacyjnego oraz nakłonienie ich do pełnego zaangażowania w trakcie wykonywania przydzielonych zadań.

Zwirtualizowane stanowisko laboratoryjne opracowano z wykorzystaniem rozwiązania firmy F5 Networks o nazwie BIG-IP. Produkt ten został wybrany ze względu na szeroki zakres funkcji, które oferuje oraz wysoką skuteczność działania, w znacznym stopniu zwiększającą poziom zabezpieczeń aplikacji internetowych. Produkt BIG-IP, pomimo dużej różnorodności realizowanych

funkcji w zakresie ochrony aplikacji internetowych, jest rozwiązaniem intuicyjnym i łatwym w konfiguracji, co potwierdza słuszność jego wyboru do celów dydaktycznych.

Co bardzo istotne, opracowane scenariusze ćwiczeń praktycznych, uwzględniające możliwości produktu BIG-IP, umożliwiają zapoznanie się ze sposobami konfiguracji tego rozwiązania, poznanie jego funkcji oraz badanie skuteczności wdrażanego systemu ochrony aplikacji webowej. Autorzy są zdania, że prawidłowa realizacja przygotowanych scenariuszy pozwala na zrozumienie istoty problemu związanego z występowaniem podatności na ataki w aplikacjach webowych oraz sposobów ich eliminacji lub co najmniej znaczącej redukcji.

Literatura

[1] ANTCZAK M., ŚWIERCZYŃSKI Z., *Metodyki testowania bezpieczeństwa aplikacji internetowych*. Przegląd Teleinformatyczny, nr 2 (35), 2013, s. 13-38.

[2] ANTCZAK M., ŚWIERCZYŃSKI Z., *PTER – metodyka testowania bezpieczeństwa aplikacji internetowych*. Przegląd Teleinformatyczny, nr 1-2 (37), 2014, s. 35-68.

[3] BIAŁAS A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Wydawnictwa Naukowo-Techniczne, Warszawa, 2007.

[4] DHANJANI N., CLARKE J., *Bezpieczeństwo sieci. Narzędzia. Tworzenie i stosowanie narzędzi do testowania zabezpieczeń*. Helion, Warszawa, 2006.

[5] HOPE P., WALTER B., *Testowanie bezpieczeństwa aplikacji internetowych. Receptury*. Helion, Gliwice, 2010.

[6] PATKOWSKI A.E., *Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych*. Biuletyn Instytutu Automatyki i Robotyki WAT, nr 24, 2007, s. 63-96.

[7] ANTCZAK M., *Metodyka oraz dedykowany system służący do wykonywania testów bezpieczeństwa aplikacji internetowych (WWW).* Praca dyplomowa. Wojskowa Akademia Techniczna, 2012.

[8] F5 Networks © 2016, *Configuration Guide for Local Traffic Manager*.

[9] Norma ISO 15408, Common Criteria.

[10] OWASP Foundation © 2011, *Application Security Verification Standard 3.0*, https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf, [dostęp: 10-05-2017].

[11] Polska Norma PN-ISO/IEC 27001:2014.

[12] Polska Norma PN-ISO/IEC 27002:2014

[13] Strona F5 Networks © 2016 [online]. „*Products BIG-IP*”, [dostęp: 10.05.2017]. https://f5.com/Products/BIG-IP

[14] Strona OWASP Foundation © 2011 [online]. „*Category: OWASP Testing Project*”, [dostęp: 10.05.2017]. https://www.owasp.org/index.php/OWASP_Testing_Project

[15] Strona OWASP Foundation © 2011 [online]. „Category: OWASP Top Ten Project”, [dostęp: 10.05.2017]. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Methodology of training in the protection of web applications against attacks from cyberspace

ABSTRACT: The paper presents assumptions of the authorial methodology to conduct trainings in the field of web application protection against cyber-attacks. In addition, a laboratory stand with example training scenarios is described, that was prepared especially for an implementation of the practical part of the methodology. From a didactical point of view, it is a coherent whole, allowing knowledge transfer in a comprehensive, systematized and easily assimilable way.

KEYWORDS: internet applications security, cybersecurity, application-layer firewall

Praca wpłynęła do redakcji: 30.06.2017 r.