Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla pracowników **Dział 2, Tydzień 4** **Moduł: Złośliwe oprogramowanie i najczęstsze ataki**	
Zajęcia edukacyjne	❑ **Webinar** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	Claudio Fornaro
Cele aktywności edukacyjnej	1. Wprowadzenie do różnych typów złośliwego oprogramowania 2. Znajomość najczęściej spotykanych typów ataków
Umiejętności do zdobycia	• Podstawowa wiedza o tym, czym jest złośliwe oprogramowanie i najczęstsze ataki na systemy komputerowe Soft Skill 2 - SS2
Czas trwania okresu edukacyjnego	1 tydzień
Wymagania wstępne	***Co jest wymagane?***
	• Nie jest wymagana żadna wcześniejsza wiedza specjalistyczna

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Opis
Jeśli chodzi o złośliwe oprogramowanie, już sama nazwa sugeruje coś złośliwego. Termin ten odnosi się ogólnie do oprogramowania zaprojektowanego celowo w celu spowodowania szkód różnego rodzaju, w szczególności (ale nie tylko): blokowania usług i komunikacji, przechwytywania transmisji, kradzieży informacji prywatnych (osobistych, korporacyjnych lub rządowych) oraz tożsamości osobistej, nieautoryzowanego dostępu do informacji lub systemów, pozbawienia użytkowników dostępu do informacji. Po części wprowadzającej przedstawione są podstawowe pojęcia dotyczące złośliwego oprogramowania wraz z opisem głównych typów, zagrożeń, jakie za sobą niosą i sposobów ich ograniczania. Druga część modułu ma na celu zaoferowanie przeglądu najczęstszych ataków, na które może być narażony system, przy czym lista ta nie jest w żadnym wypadku kompletna, ponieważ każdego dnia odkrywane są nowe rodzaje ataków. Ataki te są próbami uzyskania dostępu do systemu komputerowego lub zakłócenia jego usług. Opis zaczyna się od najczęstszych i najłatwiejszych ataków (Phishing) do bardziej złożonych: Password Attacks, Buffer Overflow, SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF), File Related Attacks, Denial of Service (DoS) i Distributed Denial of Service (DDoS), Man in The Middle (MITM), ARP Spoofing lub ARP Poisoning, DNS Spoofing, Drive-by Attacks, Credential Reuse, Web Session Hijacking, TCP Session Hijacking, IP Spoofing, Zero-day Exploits oraz konsekwencje Leak of Code.

Treść materiału edukacyjnego

W informatyce "haker" i "cracker" to dwa określenia, które służą do wskazania osób posiadających dużą wiedzę na temat systemów komputerowych. Główna różnica między nimi polega na nastawieniu, z jakim działają. **Haker** (termin ten narodził się w drugiej połowie lat 1900 w MIT) działa poprzez eksplorację systemów w celu lepszego zrozumienia ich działania oraz próbując odkryć nowe wady w celu ich rozwiązania, a tym samym zwiększenia bezpieczeństwa systemu. Niektóre działania mogą być tylko demonstracyjne lub z powodów etycznych, ale nigdy z chęci zysku. Z kolei **cracker** wykorzystuje swoje umiejętności nielegalnie próbując włamać się do systemów w celu osiągnięcia zysku poprzez kradzież danych lub w sposób destrukcyjny.

Hakerzy nieustannie próbują zdobywać nową wiedzę o systemach komputerowych, aby lepiej je zrozumieć lub poprawić ich funkcje, wydajność i bezpieczeństwo. Niektórzy z nich angażują się również w działania demonstracyjne i etyczne, ale nigdy dla zysku. Działania hakerskie są wykonywane prawie zawsze bez żadnego zezwolenia, więc prawo je karze (z dużymi różnicami

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

między krajami), z tego powodu hakerzy zwykle ukrywają się za pseudonimami. Czasami mądre firmy ochroniarskie lub informatyczne zamiast ścigać hakerów, często ich zatrudniają, aby wykorzystać ich wysokie umiejętności i kreatywność (ewentualnie po spłaceniu części długu wobec Sprawiedliwości). Są wtedy zatrudniani do testowania aplikacji, systemów bezpieczeństwa i programów zarówno w produkcji, jak i już na rynku, w celu zablokowania ataków, a także zapobieżenia problemom, które mogłyby się pojawić w przyszłości z powodu błędów w systemie.

Prawdziwi hakerzy mają opinię ekspertów i są bardzo szanowani w swojej społeczności. Organizowane są konkursy, których celem jest "przebicie" systemu lub programu w jak najkrótszym czasie. Zawody te nazywane są hackathonami i często są sponsorowane przez gigantów branży komputerowej.

Termin "cracker" przypisuje się Richardowi Stallmanowi (znanej postaci ruchu wolnego oprogramowania, twórcy projektu GNU i członkowi społeczności hakerskiej od lat 70. XX wieku). Chciał on uniknąć nadużywania terminu "haker", rozróżniając kto działa bez chęci szkodzenia, a kto przeciwnie - działa w celu uzyskania zysku lub po prostu wyrządzenia szkody. Cracker to cyberprzestępca, który próbuje atakować systemy komputerowe w sposób nieuprawniony i nielegalny, ze złośliwością, próbując czerpać z nich nieuczciwe korzyści poprzez wykorzystywanie luk w zabezpieczeniach, które nie są jeszcze znane i rozwiązane. Crackerzy często zajmują się szpiegostwem przemysłowym, kradzieżą danych oraz blokowaniem sieci i stron internetowych, wandalizmem itp.

Terminy haker i cracker mają subtelne granice, które je dzielą. Na przykład, włamanie może być uznane za nielegalny akt dla niektórych ludzi, a dla innych nie, a prawo odzwierciedla te opinie; ale ten dokument nie dotyczy aspektów etycznych lub legislacyjnych. Zamiast tego, musimy wziąć pod uwagę, że dzisiaj, niestety, te dwa terminy są uważane za synonimy.

W tym dokumencie będziemy *nieszczęśliwie* używać bardziej powszechnego i nadużywanego terminu haker dla obu kategorii, będąc pewnym, że mądry czytelnik będzie w stanie odróżnić hakera od crackera.

"Hakerów" można z grubsza podzielić na kilka kategorii, najczęściej stosowane są następujące.

Black hat hakerzy wykorzystują swoją wiedzę do złośliwych lub przestępczych celów, uważając, aby nie zostać namierzonym.

White hat hakerzy testują systemy w celu zidentyfikowania możliwych luk i wyeliminowania ich, aby zapobiec niepożądanemu dostępowi. Często są to eksperci ds. bezpieczeństwa opłacani w tym celu.

Gray hat hakerzy są podobni do białych kapeluszy, ale często prowadzą badania nad lukami w systemach bez upoważnienia, a gdy te luki zostaną odkryte, wykorzystują je, aby zmusić

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

sprzedawców do naprawienia problemu, zwykle za darmo. Niektórzy sprzedawcy nagradzają ich pieniędzmi, inni ścigają ich.

Hakerzy-samobójcy (Suicide hackers) są zwykle mniej kompetentni niż czarne/białe kapelusze, ale działają z powodów ideologicznych i nie mają interesu w ukrywaniu swojej tożsamości.

Hakerzy sponsorowani przez państwo (State-sponsored hackers) są opłacani przez rząd w celu przeprowadzenia cyberataków przeciwko innemu państwu; mają dostęp do dużych zasobów zapewnionych przez państwo, jak również ochronę przed ściganiem za popełnione przestępstwa. Działają w celu odjęcia poufnych informacji, planów lub projektów, lub w celu wywołania uogólnionych zaburzeń i uszkodzenia ludności, armii, kierownictwa Rządu, szpitali, zakładów produkujących energię, wodę i zasilanie, itp. Te działania są uważane za prawdziwe działania wojenne.

Script kiddies nie mają lub jeszcze nie nabyli wielkich umiejętności, zazwyczaj korzystają ze skryptów i narzędzi stworzonych przez innych hakerów. Wszyscy hakerzy, zanim zdobędą duże umiejętności, są script kiddies.

Cyberterroryści to osoby lub grupy o wrogich zamiarach, których celem jest zazwyczaj wywołanie chaosu w danym kraju; są podobni do hakerów sponsorowanych przez państwo, ale nie mają (jeszcze) rządu, który by ich wspierał, lub wsparcie to nie jest oczywiste.

Malware - Złośliwe oprogramowanie

Malware to akronim od "**mal**icious soft**ware**", ogólnego terminu określającego każdy złośliwy program szkodliwy dla systemu. Malware to oprogramowanie, które hakerzy tworzą, aby realizować swoje cele: zarabiać pieniądze, kraść dane, zakłócać działalność itp.

Jednym z najczęstszych złośliwych programów jest tak zwany **koń trojański**[1] (lub po prostu trojan), program, który wydaje się użytecznym oprogramowaniem i często działa jako taki, ale niesie ukrytą funkcję, która jest wykonywana, aby zrobić wraz z normalnym aktywowanym po uruchomieniu aplikacji. Są to często programy shareware lub cracked programy, które są dystrybuowane zmodyfikowane w celu przeprowadzenia konia trojańskiego. W innych przypadkach jest to po prostu złośliwe oprogramowanie z mylącą nazwą, która sprawia, że wydaje się ono użytecznym oprogramowaniem. Trojany są często rozprzestrzeniane przez e-maile lub przez pobieranie programów przez sieć i zazwyczaj nie rozprzestrzeniają się same na inne komputery. Przykłady złośliwego kodu to *keyloggery* (programy, które kradną hasła i wysyłają je do hakera), *backdoory* (programy, które działają jako serwer terminali i pozwalają zdalnemu hakerowi uzyskać dostęp do komputera w pewien sposób omijając normalne procedury

[1] Termin ten wywodzi się ze starożytnej greckiej historii o koniu trojańskim, który został użyty do najazdu na miasto Troja w podstępny sposób.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

uwierzytelniania), *cryptominery* (programy, które wydobywają kryptowalutę), *boty* (skrót od robotów, używany np. do rozproszonego ataku denial of service).

Rootkity to oprogramowanie instalowane przez złośliwe oprogramowanie, które próbuje ukryć przed wykryciem obecność samego malware; osiągają to poprzez modyfikację systemów operacyjnych.

Złośliwe oprogramowanie, które infekuje inne oprogramowanie, może być wirusem lub robakiem. Te otrzymują swoją nazwę od sposobu, w jaki się rozprzestrzeniają, a nie od konkretnych typów zachowań. **Wirus komputerowy** to oprogramowanie podobne do konia trojańskiego, ale może wytwarzać kopie samego siebie poprzez infekowanie (wprowadzanie się do) innego oprogramowania, w tym plików systemu operacyjnego. Wirus rozprzestrzenia się na inne systemy, gdy zainfekowane oprogramowanie jest kopiowane i uruchamiane w tych systemach.

Podobny do wirusa jest **Robak**, jest to samodzielne oprogramowanie, które działa na komputerze i infekuje inne komputery poprzez sieć, ale bez infekowania plików.

Ransomware to rodzaj złośliwego oprogramowania, które ogranicza dostęp do zainfekowanego przez siebie urządzenia, wymagając zapłacenia okupu w celu usunięcia ograniczenia. Główne typy ransomware to 1) *Screen-locking ransomware*, które blokuje ekrany z zastraszającym oskarżeniem o nielegalne zachowanie i żądaniem od ofiar uiszczenia opłaty; 2) *Encryption-based ransomware*, gdzie złośliwe oprogramowanie niektóre rodzaje plików (zdjęcia, dokumenty) lub wszystkie pliki na zainfekowanym komputerze. Po wykonaniu pełnego szyfrowania, wyskakujące okienko zwykle informuje użytkownika, że (wszystkie) pliki zostały zaszyfrowane i że aby je odzyskać, należy uiścić opłatę, zwykle w kryptowalucie. Przykładami ransomware opartego na szyfrowaniu są CryptoLocker i WannaCry. Wariant znany jako **Wiper** wygląda jak ransomware, ale po prostu niszczy dane, nawet jeśli często wymagana jest zapłata.

Greyware to inna kategoria złośliwego oprogramowania: programy te mogą pogorszyć wydajność komputerów i mogą powodować zagrożenia bezpieczeństwa, zachowują się w sposób irytujący lub niepożądany, ale zazwyczaj są mniej niebezpieczne (co jest opinią względną) niż poprzednie kategorie złośliwego oprogramowania. Spyware (np. keyloggery, programy rejestrujące wszystkie klawisze naciskane na klawiaturze), adware (okna reklamowe na ekranie lub w przeglądarce, nieuczciwe dialery itp.), Potencjalnie niechciane programy (PUP, aplikacje, które użytkownik zainstalował tylko z powodu błędu w oknach umowy podczas instalacji innego programu) są typową formą greyware. Mogą to być samodzielne programy lub wtyczki do innych programów, na przykład przeglądarek. Czasami ograniczają się do zmiany ustawień innych programów, na przykład w celu przeniesienia użytkownika na konkretną stronę z reklamami lub pokazywania strony z reklamami przy każdym uruchomieniu przeglądarki lub od czasu do czasu.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Antywirusy

W miarę jak silniki antywirusowe zwiększają swoje możliwości wykrywania złośliwego oprogramowania, stosowana jest kombinacja różnych technik, aby spróbować uniknąć wykrycia i analizy. Nowsze złośliwe oprogramowanie jest w stanie przyjąć wyrafinowane środki zaradcze, takie jak:

- analizowanie i wykrywanie poprzez fingerprinting środowiska w celu przyjęcia określonych metod ukrywania;
- próby obfuskacji w celu zmylenia wykrywania antywirusowego opartego na sygnaturze złośliwego oprogramowania
- przyjęcie uniku opartego na czasie w celu oszukania wykrycia anomalnego zachowania, złośliwe oprogramowanie jest zwykle spokojne i aktywuje się w bardzo określonych okresach (na przykład podczas procesu rozruchu) lub po wykonaniu określonych czynności przez użytkownika.

Bardzo trudną do odkrycia techniką unikania jest *Fileless malware* lub *Advanced Volatile Threats*. Ten rodzaj złośliwego oprogramowania działa w pamięci i nie wymaga pliku do działania. Do wykonywania swojej aktywności wykorzystuje istniejące narzędzia systemowe. Brak jakiegokolwiek pliku w systemie plików sprawia, że są one dość trudne do wykrycia i analizy, z wyjątkiem, częściowo, tych narzędzi monitorujących, które sprawdzają wykorzystanie zasobów i zachowanie systemu. Wzrost liczby tego typu ataków jest bardzo duży.

Zagrożenia

Wrażliwe oprogramowanie może zostać wykorzystane do uzyskania uprawnień lub obejścia zabezpieczeń, dopóki problem nie zostanie załatany; jest to główny powód, dla którego oprogramowanie powinno być aktualizowane, w szczególności system operacyjny. Zapory ogniowe i systemy wykrywania włamań monitorują wzorce ruchu w sieci LAN.

Zasada najmniejszych uprawnień mówi, że użytkownicy i programy nie powinny mieć więcej uprawnień niż potrzebują, w przeciwnym razie złośliwe oprogramowanie może to wykorzystać.

Łagodzenie skutków

Oprogramowanie antywirusowe blokuje i ewentualnie usuwa niektóre rodzaje złośliwego oprogramowania, może zapewnić ochronę w czasie rzeczywistym przed instalacją złośliwego oprogramowania na komputerze oraz pełne skanowanie plików i konfiguracji (np. rejestru systemu Windows) w poszukiwaniu potencjalnych zagrożeń.

Osobiste zapory sieciowe analizują każde połączenie sieciowe i potrafią dostrzec nietypową

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

aktywność.

Sandboxing to uruchomienie aplikacji odizolowanej od reszty systemu, w niektórych aplikacjach można uruchomić konkretną aplikację, natomiast w bardziej złożonych systemach bardziej odpowiednia może być maszyna wirtualna.

Skanowanie podatności stron internetowych jest wykonywane przez niektóre programy antywirusowe w odniesieniu do listy znanych niebezpiecznych stron i uniemożliwia połączenie z nimi.

Segregacja sieci dzieląca sieć na części i umożliwiająca tylko ten ruch między nimi, który jest znany jako legalny, co zapobiega rozprzestrzenianiu się złośliwego oprogramowania w sieci. Nowoczesne techniki Software Defined Networking są w stanie zrealizować taką segregację.

"Air gap" to sieć fizycznie izolowana lub inaczej sieć równoległa ("parallel network") wprowadza segregację sieci do granic możliwości poprzez całkowite odizolowanie części sieci i zapewnienie zwiększonej kontroli nad wejściem i wyjściem oprogramowania i danych ze świata zewnętrznego. Nawet to rozwiązanie nie jest ostateczne, ponieważ oprogramowanie i dane muszą wchodzić do izolowanego systemu, na przykład w celu łatania. Znanym przykładem naruszenia izolowanej sieci jest słynne złośliwe oprogramowanie **Stuxnet**, które zostało wprowadzone do środowiska docelowego poprzez dyski USB "przypadkowo" zapomniane w pobliżu, podniesione przez pracowników zakładu i włożone do komputerów zakładowych w celu zapoznania się z ich zawartością. Stuxnet składa się z trzech modułów: robaka sterującego atakiem; pliku linkującego, który automatycznie wykonuje robaka po włożeniu do komputera z systemem Windows; oraz komponentu rootkit odpowiedzialnego za ukrywanie wszystkich złośliwych plików i procesów, aby uniemożliwić ich wykrycie. Inne sposoby przekraczania szczelin powietrznych analizują emisje elektromagnetyczne, termiczne i akustyczne.

Most Common Types of Attacks

Poniższa część opisują niektóre z najczęściej spotykanych ataków na system komputerowy. Lista ta nie jest i nie może być kompletna, gdyż różnorodność ataków jest niezwykle ogromna, każdy z nich ma wiele wariantów, a wiele ataków i wariantów jest tworzonych i odkrywanych (oraz rozwiązywanych) każdego dnia. Oznacza to, że celem tej części nie jest przedstawienie pełnej klasyfikacji, ale danie wyobrażenia o wysokim poziomie wiedzy wymaganej zarówno do popełniania, jak i odpierania ataków.

Phishing

Ataki phishingowe są bardzo powszechne i łatwe do przeprowadzenia. Polegają one na wysyłaniu wiadomości e-mail, które wydają się pochodzić od wiarygodnego nadawcy, takiego jak kolega z

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

pracy lub bank, w celu nakłonienia ofiary do wykonania określonej operacji.

Atakujący próbuje nakłonić ofiarę do otwarcia załącznika lub podaje link, który prowadzi do strony bardzo podobnej do oryginalnej, np. strony głównej banku, ale stworzonej przez atakującego, a następnie prosi ofiarę o podanie swoich danych uwierzytelniających. Do optymalizacji tego typu ataku służą techniki należące do tzw. inżynierii społecznej, ponieważ w tym przypadku podatność systemu komputerowego ma być zidentyfikowana w samym użytkowniku, który zostaje oszukany i nieświadomie podaje swoje dane uwierzytelniające.

Aby obronić się przed tymi atakami, konieczna jest dokładna inspekcja linku (prawie niemożliwe jest odróżnienie małej litery L "l" od cyfry jeden "1", czy zauważenie różnicy między .it i .lt w adresie URL). Ponadto, należy mieć świadomość, że poważne firmy nigdy nie umieszczają w swojej poczcie elektronicznej linków, które przenoszą na stronę logowania.

Ataki na hasła (Password Attacks)

Aby uzyskać hasła od ofiary, haker może spróbować inżynierii społecznej, jak widać w poprzednim akapicie, lub przeprowadzić atak na hasło. Hasła są zwykle przechowywane jako hashe, a hashe są bardzo trudne do odwrócenia. Istnieją zasadniczo dwa przypadki: zaszyfrowane hasło jest dostępne lub jest nieznane i ten rodzaj ataku można przeprowadzić na różne sposoby:

- **Atak brute force**: w tym przypadku program będzie próbował wszystkich możliwych kombinacji znaków z zestawu;
- **Atak słownikowy**: program przetestuje ciąg powszechnie używanych haseł (słownik);
- **Atak za pomocą plików tęczowych**: tabela tęczowa jest wstępnie obliczoną tabelą zawierającą dane wyjściowe funkcji haszujących wykorzystywanych do tworzenia haseł.

Zarządzający systemami powinni regularnie testować pliki z hasłami użytkowników swoich systemów za pomocą programów zdolnych do przeprowadzania ataków na hasła, zarówno metodą brute force, jak i słownikową.

Aby zabezpieczyć się przed tymi atakami, system powinien testować jakość hasła przed dopuszczeniem użytkownika do jego ustawienia, wymuszając użycie minimalnej liczby znaków (np. 10) z różnych zestawów (duże i małe litery, cyfry, znaki interpunkcyjne). Jeśli zaszyfrowane hasło jest nieznane, należy przyjąć politykę blokady konta lub opóźnienia po kilku nieważnych próbach, co uniemożliwi atakującemu wypróbowanie wielu kombinacji.

Przepełnienie bufora (Buffer Overflow)

Przepełnienie bufora (lub przekroczenie) występuje, gdy wysyłasz więcej danych do bufora niż może on pomieścić, dane przepełniają bufor przeznaczony do ich przechowywania i zmieniają inne dane lub, w zależności od systemu operacyjnego i typu pliku, nawet wstrzykują wykonywalny kod

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

maszynowy. Podczas gdy nowoczesne systemy operacyjne mogą zapobiec uruchomieniu pliku wykonywalnego z mieszanymi danymi i kodem, nie jest to prawdziwe dla prostszych systemów operacyjnych często spotykanych w systemach wbudowanych, gdzie w wielu przypadkach nie ma systemu operacyjnego w ogóle.

SQL Injection

Język SQL jest używany w relacyjnych bazach danych; dlatego też tego typu ataki mają na celu kradzież informacji. W istocie, ze względu na interpretowaną naturę zapytania SQL, złośliwy kod SQL jest wysyłany do strony internetowej, o której wiadomo, że używa zapytania SQL w celu zebrania danych do zaprezentowania użytkownikowi. Złośliwy kod SQL modyfikuje (czasami tylko dodając inne części składowe) predefiniowane zapytanie SQL, w wyniku czego powstaje zmodyfikowane zapytanie, które eksponuje inne dane niż te, dla których zostało napisane oryginalne zapytanie.

Zapobieganie tego typu atakom nie jest skomplikowane (np. uniemożliwienie dostępu do innych tabel bazy danych poza tymi, które są potrzebne do wykonania oryginalnego zapytania), ale SQL injection wciąż jest jednym z najczęściej spotykanych ataków.

Cross-site Scripting (XSS)

W przypadku cross-site scripting (XSS) złośliwy skrypt wykonywalny zostaje wstrzyknięty do kodu zaufanej aplikacji internetowej (pluginu) lub strony internetowej, w wyniku czego zostaje pobrany przez inne osoby (oglądających). Gdy serwer odsyła skompromitowaną stronę internetową, przeglądarka użytkownika uznaje, że została ona dostarczona z zaufanego źródła, a wtedy wstrzyknięty kod nie jest identyfikowany jako złośliwy. Aktywna zawartość to zazwyczaj skrypt (kod programistyczny wykonywany przez przeglądarkę), który może umożliwić atakującemu uzyskanie dostępu do wrażliwej zawartości strony, ciasteczek sesyjnych lub innych informacji przechowywanych przez przeglądarkę w imieniu użytkownika. Dzięki atakom XSS możliwa jest kradzież wrażliwych danych wszystkich użytkowników, którzy wchodzą na zainfekowane strony. Na przykład, kradzież identyfikatora SESSIONID sesji strony internetowej (który znajduje się w ciasteczkach przeglądarki użytkownika, które z kolei są wykorzystywane do tego, aby każde połączenie z tą samą stroną internetową nie wymagało uwierzytelnienia poza pierwszym), może pozwolić oszustowi na ominięcie fazy logowania i nielegalne działanie w imieniu użytkownika.

Cross-Site Request Forgery (CSRF)

CSRF to wymuszone (chciane przez atakującego) żądanie http do strony internetowej wykonane przez użytkownika już uwierzytelnionego na tej stronie; strona w tym momencie wykona żądanie bez dalszej weryfikacji, umożliwiając atakującemu przeprowadzenie swojego ataku. Tego typu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

atak pozwala na modyfikację danych użytkownika lub wykonanie niepożądanych transakcji, takich jak niechciane zakupy, gdyby chodziło np. o witrynę e-commerce. Atakujący musi mieć bardzo dobrą znajomość danej strony, aby przeprowadzić atak CSRF.

Przykładowy atak CSRF jest wykonywany poprzez zmianę adresu URL. Na przykład kod źródłowy strony internetowej jest analizowany przez złośliwe oprogramowanie w celu znalezienia linku "Change password" i zweryfikowania, że użyto metody http GET, następnie można utworzyć nowy link z nowym hasłem (wybranym przez atakującego) i wysłać go do ofiary, na przykład za pośrednictwem załącznika do wiadomości e-mail. Jeśli link zostanie kliknięty i okaże się, że ofiara jest już uwierzytelniona na stronie internetowej, uruchamiany jest ukryty start procedury zmiany hasła, skutecznie oddając konto hakerowi. Dobre metody zmiany hasła proszą o wstawienie starego hasła i zastosowanie metody CAPTCHA (test sprawdzający, czy użytkownik jest człowiekiem czy komputerem), która jest dość skuteczna.

Ataki związane z plikami

Istnieje wiele rodzajów ataków na pliki. Do najbardziej znanych podatności należą:

- **Niepewne bezpośrednie odniesienia do obiektu** (Insecure Direct Object References): występuje, gdy aplikacja żąda od serwera zasobu nazywając go po imieniu, ale pozwalając użytkownikowi na modyfikację tego ostatniego, w celu zażądania innego zasobu.
- **Włączanie plików lokalnych** (Local File Inclusion (LFI)): wykorzystuje lukę w funkcjach GET i POST języka PHP do umieszczenia w kodzie złośliwych plików.
- **Przeszukiwanie ścieżek** (Path Traversal): pozwala złośliwemu użytkownikowi na dostęp do katalogów z ograniczonym dostępem i wykonywanie poleceń. Często są one wykorzystywane po LFI, aby dostać się w głąb systemu i uzyskać niezbędne uprawnienia.

Aby zabezpieczyć się przed tego typu atakami, należy uniemożliwić wysyłanie plików na serwery, wyłączyć zdalne wykonywanie kodu, ograniczyć dostęp PHP do systemu plików oraz aktualizować oprogramowanie.

Odmowa dostępu - Denial of Service (DoS) oraz Distributed DoS(DDoS)

Być może najbardziej znane ataki sieciowe, ataki DoS polegają w zasadzie na wysyłaniu wielu pakietów w celu zablokowania możliwości odbioru innych pakietów, uniemożliwiając w ten sposób dostęp do maszyny zwykłym użytkownikom, blokując oferowane usługi.

Różnica pomiędzy atakiem DoS a DDoS polega na tym, że w pierwszym przypadku do przeprowadzenia ataku wykorzystywany jest pojedynczy host, natomiast w drugim atak przeprowadzany jest przy użyciu wielu hostów (zwanych zombie) jednocześnie. Hosty te zostały

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

wcześniej zainfekowane przez złośliwe oprogramowanie i na polecenie atakującego rozpoczynają połączenie z maszyną ofiary.

Spośród ataków DoS możemy zapamiętać:

- **Syn-Flood**: polega na wysyłaniu dużej ilości żądań połączenia. Maszyna, która otrzyma żądanie (pakiet SYN) od klienta, odpowie mu wysyłając wiadomość, przydzielając pewne zasoby dla tego połączenia i czekając na pakiet potwierdzający (który nigdy nie nadejdzie). Dlatego żądanie połączenia pozostaje aktywne do momentu wystąpienia **timeoutu**. Jeśli wszystkie możliwe połączenia zostały uruchomione, usługa świadczona przez maszynę nie będzie już dostępna. Timeout następuje w ciągu kilku sekund, ale ogromna liczba żądań sprawia, że maszyna jest zapchana.
- **Smurf**: ten atak jest połączeniem spoofingu IP i żądań ICMP. IP spoofing odnosi się do wysyłania pakietu IP, w którym IP nadawcy jest sfałszowane. Poprzez ciągłe wysyłanie *żądań ICMP echo* (komunikat wysyłany przez polecenie ping, używany do sprawdzenia, czy maszyna jest osiągalna) na rozgłaszane adresy IP po zastąpieniu adresu IP nadawcy adresem IP ofiary, maszyna ofiary otrzyma odpowiedź na każde żądanie od każdego hosta aktywnego w sieci, blokując w ten sposób połączenie (flood). Aby zapobiec takim atakom można wyłączyć w routerach przekazywanie adresów IP typu broadcast.
- **Ping of death**: polega na wysłaniu do maszyny-ofiary pofragmentowanego pakietu o całkowitym rozmiarze IP większym niż maksymalny dopuszczalny, po ponownym złożeniu pakietu przez maszynę może dojść do przepełnienia bufora.

Częstym zjawiskiem w atakach DDoS jest wykorzystanie **botnetu**, czyli tysięcy lub milionów komputerów zainfekowanych złośliwym oprogramowaniem, które na polecenie atakującego wykonują jednomyślnie atak Syn-Flood na serwer ofiary.

Człowiek w środku - Man in The Middle (MITM)

Przez MITM rozumiemy całą typologię ataków, których celem jest przechwycenie, analiza i retransmisja komunikacji pomiędzy dwoma stronami, które sądzą, że komunikują się bezpośrednio ze sobą.

Ten rodzaj ataku przeprowadzany jest zazwyczaj przy użyciu spoofingu IP: sniffery sieciowe podsłuchują połączenie i nowe pakiety tworzone poprzez zmianę adresu IP nadawcy i odbiorcy tak, że nadawca wysyła dane do atakującego, który z kolei przesyła je ponownie do odbiorcy i odwrotnie.

W celu obrony przed tego typu atakami jednym z najskuteczniejszych środków zaradczych jest przyjęcie *szyfrowania end-to-end*, gdzie podmioty końcowe wykonują szyfrowanie/deszyfrowanie, a wszystkie systemy pośrednie widzą tylko zaszyfrowane dane.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

ARP Spoofing lub ARP Poisoning

Protokół ARP (Address Resolution Protocol) umożliwia komunikacji sieciowej dotarcie do konkretnego urządzenia w sieci lokalnej. Służy on do mapowania adresów IP na adresy Media Access Control (MAC) (używane do identyfikacji hostów w sieci LAN). Aby połączyć się z Internetem, host musi użyć protokołu ARP, aby poznać adres MAC routera/bramy. Każdy host utrzymuje **pamięć podręczną ARP**, aby mapować już żądane i znane pary IP/MAC. Jeśli host nie zna adresu MAC dla pewnego lokalnego adresu IP, wysyła pakiet żądania ARP broadcast, pytając wszystkie inne hosty w sieci lokalnej, kto ma ten adres IP. Host posiadający ten adres IP odpowie, podając tym samym swój adres MAC.

Atak ARP spoofing/poisoning można sklasyfikować jako atak MITM w sieci lokalnej. Atakujący musi mieć dostęp do sieci lokalnej i skanuje ją w celu ustalenia adresów IP routera i innego hosta. Atakujący wysyła sfałszowane odpowiedzi ARP, które sprawiają, że router i host wierzą, że adres MAC atakującego jest adresem odpowiednio hosta i routera. W ten sposób oszukuje zarówno router, jak i stację roboczą, aby połączyły się z maszyną atakującego, zamiast ze sobą. Ponieważ oba urządzenia aktualizują swoje wpisy w pamięci podręcznej ARP, host i router komunikują się z atakującym zamiast bezpośrednio ze sobą.

DNS Spoofing

Domain Name System (DNS) to system nazewnictwa używany do konwersji nazw internetowych (bardziej poprawnie FQDN - Fully Qualified Distinguished Names, np. www.server.net) na odpowiadający im adres IP. System ten jest hierarchiczny i zdecentralizowany z kilkoma serwerami najwyższego poziomu. Za każdym razem, gdy system próbuje dotrzeć do zasobu sieciowego, nawiązywane jest połączenie z serwerem DNS w celu konwersji nazwy zasobu na adres IP. Rekordy zasobów zawierają zwykle informacje administracyjne i inne dane wykorzystywane np. przez serwery pocztowe.

Haker będzie chciał zmienić rekordy DNS, aby wysłać ruch do fałszywej lub "spoofed" strony internetowej zamiast legalnej. Zafałszowana maszyna (spoofed) może następnie wykonać ataki MITM, spoofing, itp. Aby zapobiec spoofingowi DNS, serwery DNS muszą być aktualizowane.

Ataki typu „Drive-by”

W ataku drive-by złośliwy kod jest osadzony na niezabezpieczonej stronie internetowej. Kiedy zainfekowana strona jest odwiedzana, skrypt jest automatycznie wykonywany na komputerze ofiary i kompromituje go, nie ma potrzeby robienia czegokolwiek na stronie lub wprowadzania jakichkolwiek informacji. W tym przypadku użycie aktualnego i porządnego programu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

antywirusowego i/lub osobistej zapory sieciowej jest jedyną ochroną, ponieważ mogą one wykryć, czy strona jest niebezpieczna, zanim użytkownik odwiedzi ją ze swojej bazy danych.

Ponowne wykorzystanie poświadczeń

Konieczność posiadania danych uwierzytelniających do kilku usług sprawia, że użytkownicy ponownie używają niektórych swoich haseł. Gdy atakujący posiada listę nazw użytkowników i haseł skompromitowanych stron lub usług (na przykład uzyskaną z Dark Web), możliwe jest, że ten sam użytkownik może używać tej samej pary użytkownik/hasło w innych systemach. To znacznie ograniczy liczbę haseł do sprawdzenia przy pomocy ataku słownikowego. Aby przeciwstawić się temu rodzajowi ataku, skuteczne są te same środki zaradcze przyjęte do przeciwdziałania atakom na hasła. Gdy potrzeba wielu złożonych haseł, niektórzy uważają, że przydatne są menedżery haseł.

Przechwytywanie sesji internetowej

Atak przechwytywania sesji internetowej (Session Hijacking) polega na wykorzystaniu tokenów sesji, używanych przez przeglądarki internetowe jako mechanizmy kontroli sesji. Serwer WWW musi odnosić się do różnych połączeń od tego samego użytkownika, ponieważ dla każdej strony WWW tworzone jest połączenie TCP dla każdego elementu (tekstu, obrazów itp.). Najczęściej stosowana metoda opiera się na tokenie, który serwer WWW wysyła do przeglądarki klienta po udanym uwierzytelnieniu klienta. Token sesyjny jest tylko identyfikatorem, długim unikalnym ciągiem znaków i może być wykorzystany do uniknięcia konieczności wykonywania procedury uwierzytelniania dla każdego połączenia. Atak ten polega na kradzieży lub podrobieniu ważnego tokena sesji w celu uzyskania nieautoryzowanego dostępu do Web Servera.

Przechwytywanie sesji TCP

Połączenia TCP muszą gwarantować dostarczenie pakietów w odpowiedniej kolejności, aby to osiągnąć wykorzystuje się pakiety potwierdzające i numery sekwencyjne. Po trójstronnym wstępnym uścisku dłoni, pakiety potwierdzające są po prostu numerami, które są w jakiś sposób inkrementowane. Celem porywacza sesji TCP jest stworzenie stanu, w którym klient i serwer nie są w stanie wymieniać danych; umożliwia mu to fałszowanie pakietów akceptujących dla obu końców, które naśladują prawdziwe pakiety. W ten sposób atakujący jest w stanie uzyskać kontrolę nad sesją. Jeśli sekwencja może być przewidziana, atakujący może wysłać sfałszowane pakiety, które są rozpoznawane jako ważne z hosta ofiary.

IP Spoofing

Spofing IP jest zwykle wykonywany za pomocą ataku DoS: pewna liczba połączeń blokuje legalny

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

serwer, a fałszywy serwer ustawia swój adres IP z numerem legalnego serwera. Dlatego użytkownik jest kierowany do fałszywego serwera, który wysyła wiadomości z adresem IP wskazującym, że wiadomość pochodzi z zaufanego hosta.

Porwanie na ślepo (Blind Hijacking): W przypadkach, gdy routing źródłowy jest wyłączony, porywacz sesji może również użyć blind hijacking, gdzie wstrzykuje swoje złośliwe dane do przechwyconej komunikacji w sesji TCP. Jest to nazywane ślepym, ponieważ nie widzi odpowiedzi; chociaż porywacz może wysyłać dane lub polecenia, to w zasadzie zgaduje odpowiedzi klienta i serwera.

Exploit dnia zerowego (Zero-day Exploit)

Ściśle rzecz biorąc, **zero-day exploit** nie jest specyficznym atakiem, ponieważ cyberprzestępcy dowiadują się o luce, która została właśnie odkryta w pewnym oprogramowaniu i systemach operacyjnych, a następnie obierają za cel organizacje korzystające z tego oprogramowania, zanim poprawka stanie się dostępna.

Wyciek kodu

Kod źródłowy aplikacji może niekiedy zawierać wrażliwe informacje i dawać cenne wskazówki do cyberataku, oprócz wewnętrznej wartości ekonomicznej samego kodu.

Pytania:

W osobnym pliku.

Załączniki:

W osobnym pliku.

Odnośniki:

Każdy temat ma swoją stronę w Wikipedii, czasem już zbyt dokładną jak na potrzeby tego kursu; książki są zbyt specjalistyczne i przydają się dopiero po bardzo głębokim przeszkoleniu w danym temacie.

1. Malware, czyli złośliwe oprogramowanie.
   URL: https://www.malwarebytes.com/malware
2. Cybersecurity dla każdego.
   https://www.avast.com/c-malware
3. Czym są zagrożenia dla cyberbezpieczeństwa?
   URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

4. 21 największych zagrożeń dla bezpieczeństwa cybernetycznego i jak może pomóc Threat Intelligence
URL: https://www.exabeam.com/information-security/cyber-security-threat/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.