Referat z przedmiotu
Administracja systemami komputerowymi
Temat: Bezpieczeństwo systemu Unix

Prowadzący:
mgr inż. Bogusław Juza
Zespół:
Konrad Krzysik
Grzegorz Majka
Maciej Kołodziej

1. Firewall'e

Dostęp do poczty elektronicznej czy innych usług Internetowych jest często niezbędny do prowadzania biznesu i dostępu do informacji. Jednakże wraz z wygodą jaką przynosi dostęp do sieci, powoduje on także pojawienie się poważnych problemów z bezpieczeństwem. Przy stałych połączeniach typu DSL, czy modemach kablowych, oferujących często stały adres IP, użytkownicy są narażeni na ataki z zewnątrz, takie jak wirusy czy włamania, które mogą doprowadzić do strat np. w poufnych informacjach, czy ważnych danych, nieocenionych dla biznesu. W połączeniu z innymi rozwiązaniami, firewall może pomóc w zapobieganiu podobnym zdarzeniom.

Czym są Firewall'e?

Firewalle są narzędziami, które pozwalają na zwiększenie bezpieczeństwa przy korzystaniu z sieci, takich jak LAN, czy Internet. Firewall oddziela komputer od internetu, kontrolując pakiety danych kiedy przechodzą one przez niego, tak danych wchodzących jak i wychodzących, aby stwierdzić, czy mogę one być przesłane dalej.

Firewalle kontrolują, czy pakiety przechodzące przez niego spełniają pewne ustalone reguły, które są ustalone przez administratora filrewall'a. Działają przy tym na dwa sposoby: akceptując lub odrzucając pakiety w oparciu o listę dopuszczalnych adresów źródłowych oraz w oparciu o listę dopuszczalnych portów docelowych.

Skanowanie portów

Częstą techniką używaną przez osoby chcące dostać się do danego komputera jest skanowanie portów komputera. Narzędzia używane w tym celu wyszukują porty udostępniające typowe usługi (typu FTP, HTTP, SMTP, login, itd.). Po zlokalizowaniu portu na którym działa konkretna usługa lub aplikacja włamywacz może określić czy jest ona wrażliwa na atak. Następnie można wykorzystać różnego rodzaju exploity na daną usługę, które pozwolą dostać się do systemu. W typowym systemie jest 65535 portów, które mogą być użyte przy tego rodzaju ataku.

Statyczne filtrowanie pakietów

Najprostszą metodą działania firewall'a jest wspomniane powyżej filtrowanie pakietów. Kiedy firewall filtrujący pakiety otrzyma pakiet, sprawdza on informacje zawarte w nagłówku pakietu i porównuje z tabelą reguł kontroli dostępu, aby stwierdzić czy pakiet może zostać zaakceptowany. W tym przypadku zestaw reguł jest ustalany przez administratora firewall'a. Reguły takie mogą definiować różne akcje dla konkretnych adresów IP, podsieci lub portów (źródłowych i docelowych), oraz flag (ACK, FIN, PSH, RST, SYN, URG).
Filtrowanie UDP jest dużo trudniejsze niż filtrowanie TCP, ponieważ UDP nie zawiera tak wielu informacji, jak połączenie przy użyciu protokołu TCP. Jedynymi informacjami, które mogą być użyte do kontroli ruchu w sieci są numery źródłowe i docelowe portów. Dodatkowym utrudnieniem jest fakt, że wiele usług bazujących na UDP używa tych samych portów dla źródła oraz dla celu (np. DNS używa portów 53). Uniemożliwia to blokowanie przychodzącego ruchu na taki port, ponieważ spowoduje to blokowanie danych, które są odpowiedziami.

Pakiety ICMP nie posiadają pola numeru portu. Filtrowanie pakietów ICMP polega na sprawdzeniu zawartości pola typu i kodu. Jednak nie wszystkie filtry pakietów są dostosowane do filtrowania wszystkich typów i kodów.

Chociaż statyczne filtrowanie pakietów jest szybkie, to jest jednak stosunkowo łatwe do obejścia. Jedną z metod jest tzw. IP SPOOFING, który polega na podszyciu się pod adres IP zaufanego źródła. Drugim podstawowym problemem przy firewall'ach stosujących statyczne filtrowanie pakietów jest to, iż dopuszczają one bezpośrednie połączenia pomiędzy komputerami. Kiedy więc połączenie zostanie zatwierdzone przez firewall, komputery są łączone bezpośrednio, potencjalnie umożliwiając atak.

Dynamiczne filtrowanie pakietów (stateful packet inspection)

Drugą metodą powszechnie używaną w firewall'ach jest dynamiczne filtrowanie pakietów. Polega ono na filtrowaniu pakietów w oparciu nie tylko o ich nagłówki, ale także o zawartość, aby uzyskać więcej informacji, niż tylko adresy źródłowy i docelowy pakietu. Dynamiczny filtr wykonuje tę samą pracę co statyczny, ale dodatkowo tworzy tabelę stanów, do której wpisuje dane, gdy zostało utworzone jakieś połączenie. Za każdym razem, gdy zdalna maszyna próbuje odpowiedzieć chronionej, sprawdzana jest tabela stanów w poszukiwaniu:

- czy chroniona maszyna wysłała jakieś zapytanie,
- czy port źródłowy informacji zgadza się z odpowiedzią,
- czy port docelowy informacji zgadza się z odpowiedzią.

Kiedy pakiety FIN są przesłane przez każdy system, odpowiedni wpis w tabeli jest usuwany. Statyczne filtrowanie pakietów UDP jest bardzo trudne, ponieważ nagłówek UDP nie zawiera informacji na temat stanu połączenia. Dynamiczny filtr pakietów radzi sobie dobrze z pakietami UDP, ponieważ ma swoją własną tabelę stanów i nie polega na danych zapisanych w nagłówkach pakietów. Gdy potrzebujemy filtrowania pakietów UDP dynamiczny filtr pakietów jest bardzo zalecany.

Implementacja dynamicznego filtru pakietów jest specyficzna dla każdego typu transportu. Oznacza to, że dla każdego protokołu takiego jak TCP, UDP oraz ICMP implementacja jest inna. Dlatego podczas wyboru dynamicznego filtru pakietów należy się upewnić, że firewall obsługuje filtrowanie tego typu, którego chcemy używać.

Proxy

Ten typ ochrony pozwala na określenie czy połączenie z konkretną aplikacją jest dozwolone. Tylko połączenia dla konkretnych celów, takie jak dostęp do WWW, czy poczta elektroniczna są dopuszczalne. Pozwala to administratorowi systemu na kontrolę jakie aplikacje będą używane na komputerach sieci.

Przykładowo włamanie może polegać na próbie połączenia poprzez Telnet. Jednak firewall może być skonfigurowany do przepuszczania wyłącznie ruchu aplikacji web'owych oraz poczty elektronicznej. Może on odrzucać wszystkie pakiety na port 23. Każda próba nawiązania połączenia Telnet'owego z komputerem wewnątrz sieci nie powiedzie się, ponieważ frewall odrzuci je.

Nazwa proxy pojawia się tutaj, ponieważ firewall taki może dodatkowo służyć jako serwer proxy. Serwer proxy jest aplikacją, która przekazuje ruch między dwoma segmentami sieci. Proxy są często stosowane zamiast filtrowania, aby wstrzymać ruch bezpośredni między sieciami. Dzięki proxy, źródłowy i docelowy system nie są w rzeczywistości połączone ze sobą. Proxy stoi pośrodku każdej próby połączenia. Proxy nie wykonuje rutowania, ale wykonuje połączenia za każdy system po każdej stronie firewalla. Kiedy chcemy połączyć się z jakąś usługą na zdalnym serwerze, żądanie kierowane jest do bramy prowadzącej do zdalnej sieci, którą jest w rzeczywistości serwer proxy. Gdy proxy odbierze żądanie, identyfikuje jaki rodzaj usługi żądamy. Po identyfikacji, proxy przpuszcza żądanie do specjalnej aplikacji używanej tylko dla sesji danego protokołu. Aplikacja ta weryfikuje żądanie z listą dostępu, czy pozwolić na ten typ ruchu. Jeśli tak, proxy formułuje nowe zapytanie do zdalnego serwera z tym, że podaje siebie jako źródło. Kiedy serwer odpowiada, przesyła dane do proxy. Kiedy proxy odtrzymuje odpowiedź, kieruje ją znowu do aplikacji odpowiedzialnej za dany protokół. Kiedy informacje w odpowiedzi są akceptowalne, kierowane są do naszego komputera.

Ponieważ serwery proxy podwajają każde połączenie, możliwe jest zapisywanie (logowanie) każdego z nich. Serwery proxy są w pełni bezpieczne, gdyż nie dokonują bezpośredniego rutingu. Jedyną ich wadą są ogromne wymagania sprzętowe oraz pewien brak elastyczności. W momencie pojawienia się nowej usługi, z której użytkownicy sieci chcą skorzystać, musimy zainstalować dodatkowy program na serwerze zapewniający daną usługę.

Network adress translation (NAT)

W wolnym tłumaczeniu oznacza to translację adresów, czyli maskaradę. Działa to podobnie jak proxy, ukrywając adresy poszczególnych komputerów przed światem zewnętrznym. Wszystkie adresy konwertowane są na jeden, co powoduje, że ze świata dana sieć widoczna jest jako jeden adres IP. Rezultat jest taki, że osoba skanująca sieć

w poszukiwaniu adresów nie może zidentyfikować komputerów w sieci, ani przechwycić szczegółów o ich adresach IP, lokacji, itp.

Wady używania firewall'i

Czas na wady. Chociaż firewall'e mają dużo zalet, to jednak istnieją sposoby ataku, z którymi nie potrafią sobie poradzić, takie jak podsłuchiwanie, czy przechwytywanie poczty elektronicznej. Ponadto, podczas gdy firewall'e stanowią pojedynczy punkt ochrony i kontroli, stają się także pojedynczym punktem, w którym może nastąpić awaria. Ponieważ firewall stoi pomiędzy siecią, a światem zewnętrznym, jego uszkodzenie może spowodować utratę dostępu do sieci.

Istnieje też inne zagrożenie. O ile firewall'e mogą ochronić od większości ataków z zewnątrz, to co jeśli atak przeprowadzany jest z wewnątrz? W przypadku nieuczciwych pracowników firewall nie na wiele się zda. No i jak wspomniano wyżej w części o filtrowaniu pakietów – firewall'e nie są niezawodne. Przykładowo IP spoofing może być efektywnym sposobem obejścia zabezpieczeń.

Aby zwiększyć niezawodność firewall'i powinny one być używane w połączeniu z innymi technikami, takimi jak oprogramowanie antywirusowe, czy pakiety do szyfrowania danych.

Jak wybrać firewall?

W zależności od systemu operacyjnego, na którym chcemy aby oprogramowanie firewalla działało, mamy do dyspozycji wiele możliwości. Najbardziej znane to:

- Ipchains (ipfwadm, ipfw) - pozwala zamienić Linuxa lub FreeBSD w firewalla,
- IP Filter - oprogramowanie na FreeBSD, OpenBSD, SunOS, Solaris,
- CheckPoint FireWall-1 - najbardziej popularny komercyjny firewall, działa na systemach Windows NT, Sun Solaris, Linux i innych platformach Unix'owych,
- Novell BorderManager - działa w systemie Novell NetWare,

Dla systemów Windows 9x/Me/NT/2000 oraz Mac OS istnieją programy - prywatne firewalle (personal firewalls), które na komputerach osobistych pełnią funkcję filtru pakietów.

2. Sumy kontrolne

W odróżnieniu od firewall'i, technika wykorzystująca sumy kontrolne nie chroni przed atakiem. Pozwala ona natomiast na wykrycie ataku oraz zmian jakie w jego wyniku nastąpiły w systemie. Jednym z narzędzi umożliwiających tego typu kontrolę jest Tripwire, który jest obecnie dostępny jako OpenSource na stronie SourceForge. Na podstawie tego programu opiszemy więc technikę sum kontrolnych.

Tripwire

Tripwire jest formą wykrywania nieautoryzowanych zmian w systemie. Działa trochę jak szpiegowski trik z włosem na drzwiach, powiadamiając administratora kiedy ktoś zmieniał coś wewnątrz systemu, jednakże dopiero po włamaniu.

Tworzy on ‘bezpieczną’ (zwykle trzymaną na dysku/dyskietce z prawami tylko do odczytu, wraz z plikiem wykonywalnym tripwire) bazę atrybutów plików i katalogów (włączając np. właśnie sumę kontrolną MD5), które mogą być potem użyte do porównane z bieżącą wartością, aby sprawdzić czy plik lub katalog się zmienił. Jeżeli włamywacz włamał się do systemu i zamienił przykładowo /bin/date na wersję z trojanem, tripwire powiadomi o tym fakcie administratora.

Standardowo tripwire powinien być uruchamiany z cron’a i jego wyjście przekierowane do administratora. Plik konfiguracyjny pozwala na ustawienie, które pliki i katalogi tripwire ma monitorować i do jakiego poziomu szczegółowości. Poziom szczegółowości jest sterowany poprzez tzw. ‘ignore flags’. Przykładowo plik z logiem powinien istnieć, aczkolwiek może się zmienić jego rozmiar, czas dostępu, czas modyfikacji, czas stworzenia inode’a i zawartość. Prawa dostępu, inode, liczba linków, właściciel i grupa nie powinny się zmieniać.

Istnieją gotowe szablony dla popularnych ustawień, typu read only, log file, ignore, everything, które można dodatkowo modyfikować.

W przypadku wykrycia niezgodności tripwire może wysłać np. mail’a do administratora. Dla pełnego bezpieczeństwa można np. raporty drukować - dobry cracker mógłby usunąć mail’a, jeżeli jednak wyjście przekierowywane jest od razu na drukarkę, to nie ma możliwości zniszczenia wyniku bez fizycznego dostępu do sprzętu.

Używanie rozwiązania takiego jak tripwire ma oczywiście swoje wady. Przy każdorazowej zmianie pliku (np. konfiguracyjnego) należy odświeżać bazę danych. Można to robić dla pojedynczego pliku lub całego katalogu. Wymaga to jednak pewnej dyscypliny, aby było skuteczne.

3. Hasła

Bezpieczne hasła są podstawą efektywnej polityki bezpieczeństwa. Hasła zapewniają dostęp do systemu lub sieci tylko autoryzowanym użytkownikom. Niestety nie zawsze tak jest Hasła wymyślają zwykle te osoby, które ich później używają. Słowa, symbole czy daty tworzące hasło są zwykle w jakiś sposób związane z użytkownikiem który ich użył, tak żeby mógł je łatwo zapamiętać. I właśnie tutaj leży problem. Wielu użytkowników przedłoży wygodę nad bezpieczeństwo. Wybierają więc oni proste hasła. Podczas gdy pomaga im to je sobie przypomnieć przy logowaniu, to równocześnie powoduje, że są dużo trudniejsze do złamania. W ten sposób pierwsza linia obrony systemu staje się najsłabszą.

Jedną z rzeczy, za które powinien być odpowiedzialny administrator jest zapewnienie, aby użytkownicy byli świadomi potrzeby utrzymywania bezpiecznych haseł i jak powinno się je tworzyć. I dodatkowo zastosować rozwiązania zapewniające odpowiednią kontrolę ustawianych haseł. Można to osiągnąć sprawdzając każdorazowo nowe hasło przy jego zmianie i uniemożliwiać ustawienie zbyt prostego hasła, lub stosować narzędzia takie jak ludzie próbujący złamać hasła, czyli programu typu „password-cracker”.

Sposoby łamania haseł

Słowniki

Programy służące do łamania haseł używają różnych metod. Niektóre z nich używają słowników, czyli listy słów, lub wyrażeń, składających się z kombinacji liter, cyfr i innych symboli, które są często wykorzystywane przez użytkowników jako hasła. Próbują one użyć kolejno każdego z wyrażeń, jedno po drugim, dopóki nie znajdą poprawnej kombinacji.

Kiedy hasło zostaje złamane, umożliwia zalogowanie się na konto danego użytkownika, a więc daje dostęp do wszystkich danych, do których ma dostęp ten użytkownik. Dodatkowo włamywacz może wykorzystać konto do uzyskania praw administratora.

Sposób porównywania wyrażeń ze słownika z zaszyfrowanymi hasłami wygląda podobnie jak przy procesie logowania. Program przyjmuje tą samą metodę szyfrowania, którą zaszyfrowane jest hasło, a następnie przy jej użyciu szyfruje wyrażenie ze słownika, porównując następnie zaszyfrowane wersje.

Metoda czołgowa (brute-force)

O ile metoda słownikowa polega na szybkości i „przebiegłości”, o tyle druga metoda łamania haseł opiera się na mocy obliczeniowej i powtarzaniu. „Brute-forcing” jest prostą metodą, polegającą na porównywaniu każdej możliwej kombinacji i permutacji dostępnych znaków, dopóki nie znajdzie pasującego hasła. Metoda ta jest skuteczna i w końcu złamie każde hasło, jednakże jest bardzo wolna, ponieważ używa każdej wyobrażalnej kombinacji znaków. Przykładowo łamanie 3 literowego hasła, składającego się z liter i cyfr, wyglądało by następująco:

aaa, aab, aac, ..., aaA, aaB, aaC, ..., aa0, aa1, aa2, aa3, ..., aba, abb, abc, ...

każda z kombinacji znaków i symboli jest odpowiednio szyfrowana i porównywana z zaszyfrowanym oryginalnym hasłem.

Jak można sobie wyobrazić metoda ta jest tragicznie wolna w porównaniu z metodą słownikową. Jednakże, chociaż nie szybka, to jednak jest bardzo dokładna. Porównuje nawet bezsensowne kombinacje znaków, które nie zostały by przetestowane przez metodę słownikową.

Istnieją jeszcze techniki łączące obydwa powyższe sposoby i są to jak dotychczas metody najskuteczniejsze.

Znaczenie bezpiecznych haseł

Istnieje powiedzenie, że sieć jest tak bezpieczna, jak jej najsłabszy punkt. Według tej teorii hasła proste do odgadnięcia powinny być wyeliminowane, zanim umożliwią dostęp niechcianej osobie. Dlatego administratorzy także powinni używać programów szukających prostych haseł, aby zawczasu poinformować użytkowników o konieczności zmiany hasła.

Powinno się także mieć świadomość, że nie tylko zwykli użytkownicy są winni narażania systemu na włamanie poprzez proste hasła. Sami administratorzy, mając wiele haseł do zapamiętania, często używają jednego uniwersalnego hasła na wszystkich serwerach. Mogą także wyłączyć mechanizmy wymuszające użycie bezpiecznych haseł, w przypadku ich własnych kont. Mogą wreszcie, ułatwiając sobie pracę, pozostawiać domyślne hasła podczas instalacji nowego oprogramowania.

Sposoby zabezpieczania haseł

Pierwszym ze sposobów, używanym już chyba na każdym serwerze jest uniemożliwienie dostępu zwykłym użytkownikom do haseł w zaszyfrowanej postaci. Osiąga się to trzymając hasła w osobnym pliku bez prawa odczytu dla użytkowników. Rozwiązanie to nosi nazwę „shadow passwords".

Inną metodą jest niedopuszczenie używania prostych haseł poprzez zainstalowanie oprogramowania sprawdzającego np. „słownikowość" hasła, lub stawiającego wymagania co do ilości i grupy znaków, z których ma ono się składać (np. małe i duże litery, cyfry). Jest to może trochę denerwujące dla użytkownika, ale eliminuje możliwość ustawienia banalnego hasła. Pomocne w tym wypadku może być także narzędzie generujące poprawne hasła.