Rodzaje hakerskich ataków

Wiedza na temat luk w zabezpieczeniach systemów, którą posiadają hakerzy, daje im możliwość penetrowania odległych systemów i jedyną barierę stanowi dla nich wyłączony komputer. Zatem każda osoba wędrująca po Sieci powinna się liczyć z tym, że jej dysk zostanie splądrowany. Specjaliści-włamywacze w ciągu sekundy mogą zniszczyć wszystkie dokumenty. Zdają sobie z tego sprawę internauci, ale i tak nie podejrzewają nawet, jak wielkie szkody mogą ponieść. Beztroska i niewiedza użytkowników ułatwiają 99% włamań. W tym artykule przedstawię z skrócie sposoby ataków wykorzystywanych przez hakerów.

Przechwycenie sesji - to rodzaj ataku, który prawdopodobnie jest największym zagrożeniem dla serwerów przyłączonych do Internetu. Czasem bywa on nazywany „aktywnym węszeniem" (w odróżnieniu od omawianego wcześniej „węszenia biernego"). Chociaż sposób ten przypomina nieco podsyłanie numerów sekwencji TCP, jest groźniejszy, gdyż w tym wypadku haker zamiast odszyfrowywać adresy IP, uzyskuje dostęp do sieci i wymusza akceptację swojego adresu IP jako adresu sieciowego. Idea polega na tym, że włamywacz przejmuje kontrolę nad komputerem łączącym go z siecią, a następnie odłącza ten komputer i „oszukuje" serwer, podając się za legalnego użytkownika. Przechwytywanie w protokole TCP stanowi większe niebezpieczeństwo niż podszywanie się pod IP, ponieważ po udanym przechwyceniu haker ma na ogół dużo większy dostęp do systemu.

DoS (Denial of Service) - jest to atak mający na celu zablokowanie konkretnego serwisu sieciowego (na przykład strony WWW) lub zawieszenie komputera. Możliwe jest przesterowanie ataków DoS do bardziej skomplikowanych metod, co może doprowadzić nawet do awarii całej sieci. Niejednokrotnie hakerzy, którzy włamują się do systemów za pomocą tzw. techniki spoofingu lub redyrekcji, ukrywają swój prawdziwy adres internetowy, więc ich zlokalizowanie często staje się niemożliwe. Anonimowość ułatwia więc zdecydowanie atakowanie systemów metodą Denial of Service, co powoduje uniemożliwienie wykonania przez serwer jakiejkolwiek usługi. Jednak obecnie ataki te są już rzadko stosowane, gdyż większość administratorów odpowiednio się przed nią zabezpieczyła, co wcale nie było trudne, ale konieczne, gdyż programy umożliwiające ten typ hakowania (jest ich co najmniej kilkanaście) powodują zapchanie serwera, spowolnienie jego pracy aż do konieczności uruchomienia restartu. W przeszłości znane były przypadki zablokowania kilku tysięcy serwerów jednocześnie. Teraz oczywiście jest to niemożliwe!

„Tylne wejście" (backdoor) - to środek lub technika stosowana przez hakera do uzyskania dostępu do systemu sieciowego, utrzymania go i korzystania z niego. W szerszym znaczeniu określa się w ten sposób lukę w systemie zabezpieczeń. Dla hakera istotne jest zachowanie możliwości dostępu do raz „złamanego" systemu, również w obliczu wprowadzania nowych zapór, filtrów, serwerów proxy czy uaktualnień.

Wirusy - to bardzo przydatne do ataków z zewnątrz Sieci programy. Mogą one zostać podrzucone zwykłą drogą, np. jako program ściągnięty z Internetu, dyskietka z najnowszym upgradem do jakiegoś programu lub też mogą być dołączone do pliku tekstowego czy e-maila. Niekonsekwencja w przypadku takiego postępowania może wiele kosztować. Wirus przenika bowiem do komputera i może być przenoszony w sieci wewnętrznej wraz z nowszymi wersjami programów. Może on tkwić uśpiony długie miesiące, a po okresie uśpienia — zaatakować.

Atak na serwer poczty - to kolejny rodzaj hakerskiej działalności. Jego konsekwencją jest utrata kontroli nad przepływającą korespondencją (e-maile kierowane do konkretnej osoby mogą zostać odczytane i dostać się w posiadanie niepowołanych osób, możliwe jest także fałszowanie korespondencji i wprowadzenie w firmie dezorganizacji pracy). Ulubionymi przez hakerów sposobami atakowania są ataki na serwer główny, które prowadzą do utraty kontroli nad całą siecią, wiążą się z utratą wszystkich danych, z zakłóceniami pracy dowolnych usług sieciowych w całej firmie. Po przejęciu kontroli nad głównym serwerem możliwe jest przechwytywanie danych wędrujących wewnątrz sieci, a co za tym idzie — poznanie struktury wewnętrznej firmy. Możliwe jest fałszowanie danych przesyłanych siecią, blokowanie wiadomości przesyłanych między szefem a współpracownikami.

Podrabianie IP i DNS (spoofing) - stosowane jest głównie w celu przejęcia tożsamości stacji zaufanej, aby oszukać zabezpieczenia i uzyskać możliwość nieuprawnionej komunikacji ze stacją docelową. Gdy podrabiany jest adres IP, haker najpierw wyłącza stację zaufaną z komunikacji i dopiero w drugim kroku przyjmuje jej tożsamość. Stacja docelowa kontynuuje wówczas komunikację ze stacją nieuprawnioną. Zapoznanie z mechanizmem podrabiania IP wymaga dobrej znajomości protokołów IP i TCP oraz procedury wymiany potwierdzeń (handshaking).

Skanowanie portów w poszukiwaniu istniejących w zabezpieczeniach luk — idea sprawdzenia możliwie dużej liczby „nasłuchujących" i wybrania z nich tych, które mogą zostać zaatakowane lub w określonym celu wykorzystane — nie jest niczym nowym. Na podobnej zasadzie przeprowadzać można przegląd kodów systemu telefonicznego. Działania takie określa się terminem wardialing — polegają one na skanowaniu numerów telefonów i rejestrowaniu tych z nich, które odpowiadają sygnałem na możliwość nawiązania połączenia.

Przeciążanie (flooding) W systemie, którego interfejs sieciowy powiązany został z protokołem TCP/IP i który jest połączony z Internetem łączem stałym lub telefonicznym, część lub wszystkie usługi mogą stać się niedostępne. Pojawić się może wówczas komunikat w stylu:
„Połączenie utracone lub zerowane przez serwer".
Komunikat taki jest często symptomem ataku przeciążeniowego (flooding). Przedstawimy teraz atak SYN, gdzie haker ukierunkowuje się na komputer lub wybraną usługę TCP, taką jak na przykład usługa HTTP (port 80). Atak wymaga protokołu TCP, stosowanego przez wszystkie komputery w Internecie. Choć nie jest specyficzny dla systemu Windows NT, na nim oprzemy opis przebiegu włamania.

„Sniffery" lub „podsłuchiwacze sieciowe" - to programy, które pasywnie przechwytują i kopiują pakiety komunikacji sieciowej systemu, serwera, routera lub bramy. Pożytecznym zastosowaniem tego rodzaju oprogramowania jest monitorowanie i rozwiązywanie problemów z siecią. Używane przez hakerów sniffery „ciche" stanowią poważne zagrożenie sieci, głównie ze względu na małą wykrywalność i możliwość przeprowadzania autoinstalacji w niemal dowolnym systemie. Wyobraźmy sobie kolejny, czwarty krok w przedstawionym wcześniej przypadku — zainstalowanie w zaatakowanym systemie sniffera. Od tego momentu, jeśli sprzyja temu topologia sieci, atakowi podlega cała sieć, a nie tylko pojedynczy system .

Konie trojańskie - to szkodliwe, tworzące luki w zabezpieczeniach, programy, które rozpowszechnia się najczęściej jako oprogramowanie „podarowane" użytkownikowi komputera — program narzędziowy, żart czy wersja demonstracyjna gry. Jak pisaliśmy we wcześniejszych rozdziałach, mechanizm konia trojańskiego wykorzystuje się często do zainstalowania „tylnego wejścia" do systemu. Rosnąca obecnie liczba „zarażeń" tego rodzaju jest wynikiem prostej, technologicznej konieczności korzystania z portów. Usługi na portach o niższych numerach służą często do przechwytywania haseł, które są następnie przesyłane hakerowi pocztą elektroniczną lub udostępniane w katalogach FTP. Porty dalsze obsługują przede wszystkim programy zdalnego dostępu, umożliwiające komunikację z komputerem przez Internet, sieć, kanał VPN lub połączenie telefoniczne.

„Złamanie" strony WWW (Web page hack) - Hakerzy włamujący się na strony WWW zyskali sobie ostatnio pozycje na pierwszych stronach gazet. Przyczyniły się do tego ich znakomite „osiągnięcia" — zmodyfikowane bądź zastąpione strony NASA, Białego Domu, organizacji Greenpeace, Six Flags, Sił Powietrznych USA, Ministerstwa Handlu USA i Kościoła Chrystusa. Słynna witryna hakerów www.2600.com, udostępnia pod adresem www.2600.com/hacked_pages/ listę-archiwum historycznych i aktualnie „złamanych" witryn WWW).

Ataki wykorzystujące współużytkowane biblioteki - to ataki, które polegają skupiają się na zasadach działania współużytkowanych bibliotek stosowanych w systemie UNIX. Biblioteka taka zawiera zestaw funkcji, które system operacyjny wczytuje z pliku do pamięci RAM. Hakerzy mogą zastąpić niektóre programy biblioteki, funkcjami wykonującymi inne operacje, które umożliwią na przykład uzyskanie dostępu do sieci. Zabezpieczenie przed takimi atakami jest łatwe — należy regularnie sprawdzać spójność współużytkowanych bibliotek.

Ataki za pomocą apletów - stanowią jeden z najczęstszych sposobów atakowania systemu. Jego specyfika polega na przeprowadzeniu ataku typu „odmowa obsługi". Polega to na utworzeniu apletu, którego uruchomienie przez przeglądarkę będzie powodowało częste zatrzymania systemu, jak np.: Aplet InfiniteThreads.java i Klasa TripleTheat.java.

Ataki korzystające z haseł (PASWORD GUESSING) - są to najchętniej stosowane przez hakerów metody, które polegają na próbie włamania się do systemu przez podanie identyfikatora użytkownika i hasła. Programy takie używają słów zgromadzonych w słowniku i dlatego właśnie są znane pod nazwą ataków słownikowych. System Unix jest szczególnie na nie podatny, ponieważ — w odróżnieniu od innych systemów — zezwala użytkownikom na wielokrotne podawanie hasła.

Bibliografia:

John Chirillo *„Hack Wars. Tom 1. Na tropie hakerów"*
Dariusz Doroziński *„Hakerzy. Technoanarchiści cyberprzestrzeni"*