SIEĆ

System Wykrywania Włamań Sieciowych

FAQ

I. WPROWADZENIE

1.1 Co to jest "System Wykrywania Włamań Sieciowy(NIDS)"?

Intruzem jest ktoś (hacker czy cracker) próbujący włamać się lub nadużywać systemu. Słowo "nadużywać" jest dość szerokie i może odzwierciedlać coś poważnego jak kradzież poufnych danych z serwera, coś lżejszego jak nadużywanie systemu email np. Spam (choć dla wielu z nas jest to poważny problem). "System Wykrywania Intruzów (IDS)" jest to system dla wykrywania takich intruzów. IDS można podzielić na następujące kategorie:

system wykrywania włamań sieciowy (NIDS) monitoruje pakiety w sieci kablowej i próuje odkryć czy hacker/cracker ni próbuje włamać się do systemu (lub powoduje atak denial of service). Przykładem może być system ,który obserwuje dużą liczbę żądań połączeń TCP (SYN) do wielu różnych portów na maszynie docelowej, zatew odkrywa czy ktoś nie próbuje skanować portów TCP. NIDS może być uruchomionu albo na maszynie docelowej która obseruje swój własny ruch (zazwyczaj zaintegrowany ze stosem i samymi usługami) lub na niezależnej maszynie niograniczene obswerwującej cały ruch sieciowy (hub, router, sonda) Zwróć uwagę ,że "sieciowy" IDS monitoruje wszytkie maszyny, podczas gdy inne monitorują tylko pojedynczą maszynę (ta na której są zainstalowane)
weryfikacja integralności systemu (SIV) monitoruje system plików dla wykrywania kiedy intruz je zmienia (tym samym pozostawiając tylne drzwi). Najbardziej znanym z takich systemów jest "Tripwire". SIV może obserwować inne komponenty takie jak rejestr Windows i konfigurację chron, aby znaleźć dobrze znane podpisy. Może również wykryć kiedy zwykły użytkownik nabywa jakoś poziom uprzywilejowania roota / administratora. Wiele istniejących produktów w tym obszarze będzie rozpatrywanych bardziej jako "narzędzia" niż "kompletny" system tj coś takiego jak "Tripwire" wykrywa zmiany w komponentach krytycznego systemu, ale nie generuje alarmów w czasi rzeczywistym przy itruzie.
monitory pliku logowania (LFM) monitorują pliki logowania generowane przez usługi sieciowe. W podobny sposób do NIDS, systemy te szukają wzorców w plikach logowania, które sugerują atak intruza. Typowym przykładem będzie parser dla plików logowania serwera HTTP, które wyszukują intruzów próbujących dobrze znanych dziur bezpieczeństwa, takich jak atak "phf".
system oszustw (decoys, lures, fly-traps, honeypots) , które zawierają pseudo usługi których xelem jest emulowanie dobrze znanych dziur, aby śledzić hackera. Również proste sztuczki ze zmianami konta "administratora" , potem ustawienie atrapy konta.

1.2 Kto nadużywa systemu?

Są dwa słowa opisujące intruza: hacker i cracker. Hacker jest ogólnym terminem dla osoby która zna się na rzeczy. Łagodny hacker jest to osoba która lubi pohgrzebać w swoim komputerze aby zrozumieć jak działa. Złośliwy hacker jest to osoba która lbi dobierać się do systemów innych ludzi. Łagodny hacker chciałby aby media przestały krytykować wszystkich hackerów, a zamiast tego używały terminu 'cracker'. Niestety, nie jest to prawdopodobne. W każdym razie słowo używane w tym FAQ to "intruz", ogólnie oznaczające kogoś kto próbuje dostać się do systemów. Intruzi mogą być podzieleni na dwie kategorie:

Zewnętrzni: intruzi z zewnątrz sieci, i którzy mogą atakować twoją zewnętrzną obecność (niszczyć serwery WWW, przekazywać spam przez serwery e-mail itp). Mogą również próbować obejść firewalle atakując maszyny w sieci wewnętrznej. Intruzi zewnętrzni mogą pochodzić z Internetu, linii dial-up, fizycznego włamania lub z sieci partnerskiej (producent , klient, sprzedawca itp), która jest połączona z siecią firmową.

Wewnętrzni: intuzi którzy zgodnie z prawem korzystają z sieci wewnętrznej. Są to użytkownicy, którzy nadużywają przywilejów (np. pracownik ZUS oznaczający kogoś jako osobę martwą, ponieważ nie lubią tej osoby) lub podszywający się pod użytkowników z wyższym uprzywilejowaniem (jak wykorzystanie czyjegoś terminala). Często przytaczane statystyki mówią ,że 80% przypadków naruszeń bezpieczeństwa jest powodowanych przez intruzów wewnętrznych

Jest kilka typów intruzów, Joy riders hackują bo mogą , Wandale są zdecydowani niszczyć lub oznaczać strony WWW, Profitters są zdecydowani czerpać korzyści ze swojej działalności, takie jak kradzież danych firmowych i ich sprzedaż

1.3 Jak intruzi dostają się do systemów?
Podstawowe sposoby w jaki intruz może dostać się do systemu:

Wtargnięcie fizyczne. Jeśli intruz ma fizyczny dostęp do komputera (tj może korzystać z klawiatury lub systemu), będzie mógł z nich skorzystać. Zakres technik dla specjalnego uprzywilejowania posiada konsola, zdolność do fizycznego rozłożenia systemu i usnięcie napędu dyskowego (i odczyt/zapis na innej maszynie) Nawet ochrona BIOS jest łatwa do ominięcia: w zasadzie wszystkie BIOS'y mają hasła tylnych drzwi.

Wtargnięcie systemowe/ ten typ hackowania zakłada ,że intruz ma już konto użytkownika o niskim uprzywilejowaniu w systemie. Jeśli system nie posiada najnowszej poprawki bezpieczeństwa, istnieje duża szansa ,że intruz będzie mógł użyć znanych exploitów w celu zdobycia dodatkowych uprawnień administracyjncyh.

Wtargnięcie zdalne. Ten typ hackingu polega na tym ,że intruz próbuje przeniknąć system zdalnie przez sieć. Intruz zaczyna bez specjalnych uprawnień. Jest kilka form takiegu hackingu. Na przykład, intruz ma dużo trudniejszy czas jeżeli istnieje firewall między nią / nim i zaatakowaną maszynę.Należy pamiętać ,że sieciowy system wykrywania intruzów są przede wszystkim związany z wtargnięciami zdalnymi.

1.4 Dlaczego intruzi dostają się do systemów?
Oprogramowanie zawsze ma błędy. Administratorzy systemu i programiści nie mogą wytropić i wyeliminować wszystkich możliwych dziur. Intruzi muszą znaleźć tylko jedną dziurę dla włamania.

1.4.1Błędy oprogramownia

Błędy oprogramowania są wykorzystywane w demonach serwera, aplikacjach klienckich, systemie operacyjnym istosie sieciowym. Błędy oprogramowania mogą być sklasyfikowane w następujący sposób:

Buffer overflow: Prawie wszystkie dziury bezpieczeństwa o jakich czytałeś w prasie mają związek z tym problemem. Typowym przykładem jest programista który nie uwzględnił 256 znaków dla przechowania loginu użytkownika. Oczywiście programista myśli , że nikt nie będzie miał dłuższej nazwy. Ale hacker myśli, co się stanie jeśli wejdę pod fałszywą nazwą użytkownika, dłuższą niż to? Gdzie sobie idą te dodatkowe znaki? Jeśli hackerzy wykonają dobrze swoją pracę, mogą wysłać 300 znaków, w tym kod, który będzie wyskonywany przez serwer, i voila. Hacker znajduje te błędy na kilka sposobów. Po pierwsze, kod źródłowy dla wielu usług jest dostępny w sieci. Hackerzy stale przeglądają ten kod wuszukując programy, które mają problemy z przepełnieniem bufora. Po drugie hackerzy mogą patrzeć na same programy aby zobaczyć czy taki problem istnieje, chociaż czytanie danych asemblerowych nie jest łatwe.. Po trzecie hackerzy będą badali każde miejsce programu ,które ma wejście i spróbują przepełnić go losowymi danymi. Jeśli program się zawiesi, jest duża szansa, że

staranne zbudowanie danych wejściowych pozwoli hackerom na włamanie. Zauważ, że problem ten jest powszechny w programach napisanych w C/C++, ale rzadko w programach napisanych w Javie.

Nieoczekiwane kombinacje: Programy są zazwyczaj budowane przy użyciu wielu warstw kodu, wliczając w to podstawowy syste, operacyjny jako najniższa dolna warstwa. Intruzi często wysyłają dane wejściowe, które są bez znaczenia dla jednej warstwy, ale mają znaczenie dla innej warstwy. Najczęściej językiem dla przetwarzania danych wejściowych użytkownika w sieci jest PERL. Programy napisane w PERLu będą zazwyczaj wysyłać te dane wejściowe do innych programów do dalszej obróbki. Powszechną techniką hackerską będzie wpisanie czegoś takiego jak " | mail < /etc/passwd". Zostanie to wykonane, ponieważ PERL prosi system operacyjny o uruchomienie dodatkowego programu z tymi danymi wejściowymi. Jednak system operacyjny zatrzymuje znak " | " i uruchamia również program "mail", co powosuje ,że plik z hasłami będzie wysyłany pocztą do intruza.

Nieobsłużone dane wejściowe: Większość programów jest napisanych do obsługi poprawnych danych wejściowych. Większość programistów nie rozpatruje tego co się wydarzy kiedy ktoś wpisze dane, które nie pasują do specyfikacji.

Sytuacja wyścigu: Większość systemów dzisiaj jest "wielozadaniowych / wielowątkowych". Oznacza to, że mogą wykonywać więcej niż jeden program w jednym czasie. Jest to niebezpieczne jeśli dwa programy muszą mieć dostęp do tych samych danych jednocześnie. Wyobraźmy sobie dwa programy A i B , któe muszą zmodyfikować ten sam plik. Aby zmodyfikować plik, każdy program musi najpierw odczytać plik z pamięci zmieniając zawartość w pamięci, potem kopiuje pamięć z powrotem do pliku. Warunki wyścigu wystąpią kiedy program A odczytuje plik do pamięci, wtedy dokonuje zmian. Jednak zanim A przejdzie do zapisu pliku, program B angażuje się w pełny odczyt/modyfikację/zapis do pliku. Teraz program A zapisuje swoją kopię do tego pliku. Ponieważ program A zaczyna kopiowanie zanim B dokona swoich zmian, wszystkie zmiany B zagubią się. Ponieważ potrzebujemy uzyskać sekwencję zdarzeń w odpowiednim porządku, ytuacje wyścigu są bardzo rzadkie. Intruzi zwykle próbują tysiące razy zanim to osiągnie, i włamie się do systemu

1.4.2 Konfiguracja systemu

Błędy konfiguracji systemu mogąbyć klasyfikowane w następujący sposób:

Konfiguracja domyślna: Większość systemów jest dostarczana klientom z domyślną , łatwą w użyciu konfiguracją. Niestety "łatwa w użyciu" oznacza "łatwa do złamania". Prawie każde maszyna UNIX lub WINNT może być łatwą do złamania.

Leniwi administratorzy: Zadziwiająco wiele maszyn jest skonfigurowanych z pustym hasłem administratora root/. Dlatego ,że administratorzy są zbyt leniwi aby skonfigurować ten jeden raz i chcą aby msaszyna działała szybko przy minimalnym nakładzie sił. Niestety nigdy nie chce im się ustalić teg hasła później, umożliwiając łatwy dostęp intruzom. Jedną z pierwszych rzeczy jakie robi intruz to skanowanie w sieci wszystkich maszyn pod kątem pustych haseł.

Tworzenie dziur: Praktycznie wszystkie programy mogą być skonfigurowane do działania w trybie niezabezpieczonym. Czasmi administratorzy przypadkowo otworzą dziurę na komputerze. Przewodniki administratora sugerują aby administrator wyłączył wszystko co nie jest niezbędnie konieczne do uruchomienia na komputerze aby uniknąć przypadkowych

dziur. Należy pamiętać ,że pakiety audytu bezpieczeństwa mogą zwykle znaleźć te otwory i powiadomić o tym administratora.

Relacje zaufania: Intruzi często "skaczą z wyspy na wyspę" przez sieć wykorzystując relacje zaufania. Zaufanie sieci komputerów jest tak bezpeiczne jak ich najsłabsze ogniwo.

1.4.3 Łamanie haseł

Jest to specjalna kategoria

Rzeczywiście słabe hasła: Większość ludzi używa mion, swoich dzieci, współmałżonka, zwierzaka, modelu samochodu jako haseł. Są użytkownicy wybierający "password" lub po prostu nic. Daje to listę mniej niż 30 możliwości jakie może wpisać sam intruz.

Atak słownikowy: W przypadku niepowodzenia w powyższym , intruz może spróbować "ataku słwonikowego". W ataku tym, intruz będzie używał programu , który wypróbuje każde możliwe słowo ze słownika .Ataki słownikowe mogą być wykonane albo przez powtarzalne logowanie do systemu lub przez zbieranie zaszyfrowanych haseł i próbę znalezienia wzorca przez podobne szyfrowanie wszystkich haseł w słowniku. Intruzi zwykle mają kopię słownika języka ojczystego jak i innych języków do tego celu. Używają również dodatkowych słowników , takich jak baza danych nazw i list popularnych haseł.

Ataki brute force: Podobne do ataku słownikowego, intruz może próbować wszystkich możliwych kombinacji znaków. Krótkie 4 literowe hasło składające się z małych liter może zostać złamane w kilka minut (około pół miliona kombinacji). Dłuższe 7 literowe hasło składające się z dużych i małych liter, jak również cyfr i znaków interpunkcyjnych (10 trylionów kombinacji) może zająć miesiąc na złamanie zakładając ,że możesz wypróbować milion kombinacji na sekundę (w praktyce tysiąc kombinacji na sekundę jest najbardziej prawdopodobne dla pojedynczej maszyny)

1.4.4 Sniffowanie niezabezpieczonego ruchu

Media współdzielone: W tradycyjnym Ethernecie, wszystko co musisz zrobić to wstawić sniffer "na przewód" aby widzieć cały rucch w tym segmencie. Jest to coraz trudniejsze ponieważ większość firm przechodzi na Ethernet przełączany.

Sniffowanie serwera: Jednak w sieciach komutowanych, jeśli możesz zainstalować sniffer na serwerze (szczególnie działającym jako router), możesz prawdopodobnie użyć tej informacji do złamania komputera klienta jak również komputerów zaufanych. Na przykład, możesz nie znać hasła użytkownika, ale sniffując sesje Telnetu kiedy loguje się, podaje swoje hasło

Zdalne sniffowanie: Wiele skrzynek pochodzi z aktywnym RMON i publicznych łańcuchów komunikacyjncyh. Podczas gdy pasmo jest bardzo niskie (nie można sniffować całego ruchu) prezentuje ciekawe możliwości

1.4.5 Wady projektowe

Nawet jeśli implementacja oprgoramowania jest całkowicie poprawna pod kątem projektowym, jest jeszcze wiele błędów w samym projekcie, które prowadzą do intruzji.

Wady protokołu TCP/IP: Protokół TCP/IP został zaprojektowany zanim hacking

rozprzestrzenił się na taką skalę do dziś. W rezultacie istnieje szereg wad projektowych, które mogą prowadzić do potencjalnych zakłóceń bezpieczeństwa. Niektóre przykłady to ataki typu smurf,nieuchwytne rozłączenia ICMP, IP spoofing i floodowanie SYN. Największy problem jes ttaki ,że protokół IP , jako taki jest bardzo "zaufany": hackerzy mają wolną drogę do tworzenia i zmian danych IP bezkarnie. IPSec (IP Security) zostało stworzone dla pokonania wielu z tych wad, ale nie jest szeroko używane.

Wady projektowe UNIX: Istnieje wiele nieodłącznych wad w systemie operacyjnym Unix, które często prowadzą do włamań. Głównym problemem jest system kontroli dostępu, gdzie "root" jest przyznawany prawom administratora.

1.5 Jak intruzi uzyskują hasła?

Intruzi uzyskują hasła na kilka sposobów:

Sniffowanie czystego tesktu: Wiele protokołów (Telnet, FTP, HTTP Basic) używa haseł w postci jawnego tektu, co oznacza ,że nie są szyfrowane ponieważ przechodzą przewodami między klientem a serwerem. Intruz z analizatorem protokołu może obserwować przewody szukając takiego hasła. Nieznbyt wielki wysiłek jest potrzebny; intruz może zacząć natychmiast korzystać z tych haseł do logowania się.

Sniffowanie zazyfrowane: Większość protokołów jednak, używan jakiegoś rodzaju szyfrownia haseł. W tych przypadkach, intruz będzie musiał przeprowadzić atak słownikowy lub brute force na hasła w celu podjęcia próby deszyfracji. Należy pamiętać , że dalej nic nie wiemy o obecności intruza, a on jest całkowicie pasywny i niczego nie przenosi przewodami Łamnie haseł nie wymaga wysyłania niczego ponieważ intruz używa swojej maszyny do uwierzytelniania hasła.

Atak metodą powtórzenia: W niektóych przypadkach, intruzi nie muszą deszyfrować hasła. Mogą używać formy zaszyfrowanej aby logować się do systemów. Zazwyczaj wymaga to przeprogramowania oprogramowania klienckiego aby móc użyć zaszyfrowanego hasła.

Kradzież pliku z hasłami: Cała baza danych jest zwykle przechowywana w pojedynczym pliku na dysku. W systemie Unix, ten pli to /etc/passwd (lub jakiś mirror tego pliku) a w Windows, jest to plik SAM. Tak czy inaczej, kiedy intruz zdobędzie ten plik może uruchomić crackowanie programów (opisane powyżej) aby znaleźć słabe hasła wewnątrz pliku.

Obserwacja: Jednym z tradycyjnych problemów w bezpieczeństwie haseł jest to ,że hasła muszą być długie i trudne do odgadnięcia (aby zdecydowanie utrudnić ataki słownikowe czy brute force). Jednak takie hasła są trudne do zapamiętywania, więc użytkownicy je gdzieś zapisują. Intruzi często przeszukują miejsca pracy w celu znalezienia hasła zapisywanego na jakichś małych skrawkach papieru (zwykle pod klawiaturą). Intruzi często obserwują wpisywanie haseł zza pleców użytkownika .

Inżynieria społeczna: Powszechna (skuteczna) technika to po prostu zadzwonić do użytkownika i powiedzieć "Cześć tu Janek z Helpdesk. Staramy się wyśledzić jakieś problemy w sieci i wydaje się wychodzić z twojego komputera.Jakiego hasła używasz?" W takiej sytaucji wielu użytkowników poda swoje hasła. (Wiele korporacji ma zasady, które mówią użytkownikom aby nigdy nie podawali swoich haseł, nawet własnemu działowi Helpdesk, ale ta technika jest jeszcze skuteczna. Prostym rozwiązaniem dla Helpdesk jest zadzwonić do nowego pracownika zatrudnionego od 6 miesięcy i poprosić o hasło, a potem

skrytykowaćza udzielenie takiej informacji :-)

1.6 Jaki jest typowy scenariusz włamania?

Typowym scenariuszem może być:

Krok1: **rekonensans zewnętrzny**. Intruz będzie dowiadywał się jak najwięcej w istniejącej rzeczywistości. Będzie to robił przez wyszukiwanie publicznych informacji lub jako zwykły użytkownik. Na tym etapie na pewno nie można ich wykryć. Inttuz zrobi wyszukiwanie "whois" aby zebrać jak najwięcej informacji o sieci jako zarejestrowaną wraz z nazwą domeny (taką jak foobar.com może chadzać po tablicach DNS (używając 'nslookup', 'dig' lub innych narzędzi do transferu domen) aby znaleźć nazwy komputerów. Intruz będzie przeglądał inne publiczne informacje, takie jak publiczne strony internetowe i anonimowe strony FTP. Intruz może wyszukiwać artykuły prasowe o twojej firmie

Krok 2: **rekonesans wewnętrzny** Intruz wykorzystuje bardziej inwazyjne techniki do skanowania w poszukiwaniu informacji, ale jeszcze nie robi nic szkodliwego. Może on przechodzić przez wszystkie strony sieciowe i wyszuliwać skryptów CGI (skrypty CGI są często łatwe do zhackowania). Może zrobić "ping" aby zobaczyć które komputery są aktywne. Moze zrobić skan UDP/TCP na maszynach docelowych aby zobaczyć jakie usługi są dostępne. Uruchamiają oni narzędzia takie jak "rcpinfo", "showmount", "snmpwalk" itp aby zobaczyć co jest dostępne. W tym miejscu intruz zrobił "normalną: działalność w sieci i nie uczynił czegoś co można uznać za włamanie. W tym momnecie NIDS będzie mógł powiedzieć ,że "ktoś sprawdza klamik u drzwi", ale nikt nie próbował jeszcze otwierać drzwi.

Krok 3 **exploit** Intruz przekracza linię i zaczyna wykorzystywać dziury na maszynach docelowych. Intruz może próbować podjąc próbę dobrania się do skryptu CGI przez wysłanie polecenia powłoki w polach wprowadzania danych. Intruz może podjąć próbę wykorzystania znanych dziur przepełnienia bufora przez wysłanie dużej ilości danych. Intruz może zacząć sprawdzanie logowania kont łatwych do odgadnięcia (lub pustego) hasła. Hacker może przejść przez kilka etapów wykorzystywania. Na przykład, jeśli hacker miał dostęp do konta użytkownika, będzie próbował dalej wykorzystywać exploity w celu uzyskania dostępu root/administratora.

Krok 4 **przyczółek** Na tym etapie hacker pomyślnie uzyskał przyczółek w twojej sieci przez zhackowanie komputera. Głównym celem intruza jest ukrycie dowodów ataku i upewnienie się ,że może wrócić później. Może zainstalować "narzędzia" które dają im dostęp , zastąpienie istniejących usług swoimi własnymi koniami trojańskimi, które mają tylne drzwi dla haseł , lub tworzyć swoje własne konta użytkownika. Weryfikacja Integralności Systemu (SIV) mogą często wykrywać intruza w tym momencie przez odnotowanie zmian w systemie plików. Hacker będzie korzystać z systemu jako odskoczni do innych systemów, ponieważ większość sieci mam mniejszą odporność na ataki z wewnątrz.

Krok 5 **korzyści** Intruz wykorzystuje swój status do kradzieży poufnych danych, nadużycia zasobów systemu, lub wymazanie stron WWW

Inny scenariusz zaczyna się inaczej. Zamiast ataku na określoną stronę, intruz może po prostu skanować losowo adresy internetowe szukając konkretnych dziur. Na przykład, intruz może próbować skanować cały Internet dla komputerów, które mają dziurę SendMail DEBUG. Po prostu wykorzystują takie maszyny, które znaleźli. Oni nie celują w ciebie bezpośrednio, i tak naprawdę nie wiedzą kim jesteś. (jest to znane jako "atak urodzinowy"; podana jest lista dobrze znanych dziur bezpieczeństwa i lista adresów IP, i istnieje szansa ,że jakieś urządzenie ma którąś z tych dziur)

1.7 Jakie są powszechne "podpisy włamań?

Są trzy typy ataków:

rekonesans: Obejmuje pingowanie, transfer strefy DNS, rekonensans e-mail, skanowanie portów TCP lub UDP, i możliwe indeksowanie serwerów publicznych stron dla znajdowania dziur cgi.

exploit Intruzi będą korzystać z ukrytych funkcji lub błędów, aby uzyskać dostęp do systemu
ataki denial of service Intruz próbuje zawiesić usługi (lub komputer), przeciążyć łącza sieciowe, przeciążyć CPU lub przepełnić dysk. Intruz nie próbuje uzyskać informacji, ale po prostu działa jak wandal aby uniemożliwić korzystanie z komputera.

1.8 Jakie są najczęstsze exploity?

1.8.1 Skrypty CGI

Programy CGI są notorycznie niebezpieczne. Typowe dziury bezpieczeństwa obejmują przekazywanie skażonych danych wejściowych bezpośrednio do interpretatora poleceń przez wtkorzystanie metaznaków powłoki, używając ukrytych zmiennych określających nazwy plików w systemie, ujawniając więcej o systemie niż to wymagane. Najbardziej znanym błędem CGI jest biblioteka "phf" dostarczana z NCSA httpd. Biblioteka "phf" ma umożliwić parsowanie serwera HTML, ale może być wykorzystywana dla pobrania dowolnego pliku. Inne dobrze znane skrypt CGI, jaki może wypróbować intruz to : TextCounter, GuestBook, EWS, info2www, Count.cgi, handler, webdist.cgi, php.cgi, files.pl, NPH-test.cgi, nphpublish ,AnyForm, FormMail. Jeśli widzisz kogoś kto próbuje uzyskać dostęp do jednego lub wszystkich tyhc skryptów CGI (a nie używasz ich), wtedy jest to wyraźne wskazanie na próbę włamania (zakładając ,że nie masz zainstalowanej wersji jakiej faktycznie chcesz używać)

1.8.2 Ataki na serwer WWW

Oprócz wykonywania skrytpów CGI, serwery sieciowe mają inne możliwe dziury. Duża liczba samodzielnie napisanych serwerów (w tym IIS 1.0 i NetWare 2.x) mają dziury w któych nazwa pliku może zawierać szereg "../" w nazwie ścieżki przenoszony gdzieś w systemie plików, uzyskujemy dowolny plik. Innym częstym błędem jest przepełnienie bufora w żądanym polu lub w jednym z innych pól HTTP. Serwer WWW często ma błędy powiązane z ich interakcją z systemem operacyjnym. Stara dziura w Microsoft IIS wynika z faktu ,że pliki mają dwie nazwy, nazwę długą i krótką w postaci 8.3, które mogą być dostępne z pominięciem uprawnień. NTFS ma funkcję nazwaną "alternatywny strumień danych", który jest podobny do danych Macintosha i zasobów. Można uzyskać dostęp do pliku poprzez nazwę strumienia przez dodanie "::$DATA" aby zobaczyć skrypt zamiast go uruchamiać. Serwery już od dawna miały problemy z URL'ami. Na przykład "śmierć przez tysiąc slashy" problem w starszych Apache'ach spowodowałaby ogromne obciążenie procesora, ponieważ próbuje przetwarzać każdy katalog w tysiącach slashy URL'a

1.8.3 Ataki na przeglądarkę

Wydaje się ,że przeglądarki Microsoft i Netscape mają dziury bezpieczeństwa . Dotyczy to ataków na URL, HTTP, HTML, JavaScript,ramki, Javę i ActiveX

Pola URL mogą powodować przepełnienie bufora,albo jest parsowany w nagłówku HTTPm ponieważ jest wyświetlany na ekranie, albo przetwarzany w jakiejś postaci (np zapisane w historii pamięci podręcznej). Również stary błąd z Internet Explorerem pozwala na interakcję z błędem, według którego przeglądarka będzie wykonywała polecenia .LNK lub .URL
Nagłówki HTTP mogą być używane do wykorzystywania błędów ponieważ niektóre pola są przekazywane do funkcji, które oczekują tylko na pewne informacje.
HTML może być wykorzystywany, tak jak w typie MIME w Netscape Communicator, poleceniem <EMBED>

JavaScript jest od wielu lat ulubiony i zazwyczaj próbuje wykorzystać funkcję "przesłania pliku" przez generowanie nazwy pliku i automatyczne ukrywanie przycisku "Wyślij". Istnieje wiele odmian tego poprawionego błędu, a następnie znaleźć nowe sposoby na obejście poprawki.

Ramki są często stosowane jako część hackowania JavaScript lub Javy (na przykład ukrywanie stron internetowych na ekranie o rozmiarze 1px na 1px)m ale stanowią one szczególne problemy. Na przykład,mogę umieścić link do zaufanej witryny, która używa ramek, potem zastąpić niektóre z tych ramek storn swoją własną stroną, i pojawią się jako część tej zdalnej strony.
Java posiada rozbudowany model bezpieczeństwa, ale ten model ma sporadyczne błędy (chociaż w porównaniu z innymi elementami systemu, jest jednym z najbezpieczniejszych z nich) Ponadto, jego bezpieczeństwo może być zgubne: Normalne aplety Javy nie mają dostępu do lokalnego systemu, ale czasami będą bardziej przydatne jeśli nie będą miały takiego dostępu. Tak więc, zaimplementowane "zaufane" modele mogą być dużo łatwiejsze do zhackowania.
ActiveX jest jeszcze bardziej niebezpieczny niż Java, ponieważ działa wyłącznie w zaufanym modelu i uruchamia kod natywny. Można nawet przypadkowo złapać wirusa, przypadkowo osadzonego w kodzie przez sprzedawcę.

1.8.4 Ataki SMTP (SendMail)

SendMail jest niezwykle skomplikowany i powszechnie wykorzystywanym programem i w konsekwencji, był częstym źródłem luk w zabezpieczeniach. W dawnych czasach (w 1988 roku Morris Worm) hackerzy wykorzystali lukę polecenia DEBUG lub ukrytej funkcji WIZ dla włamania na serwer SMTP. Obecnie są to często próby przepełnienia bufora. SMTP może być również wykorzystywany w atakach rozpoznawczych, tak jak użycie polecenia VRFY dla znajdowania nazwy użytkownika.

1.8.5 Dostęp

Nieudane próby logowania, nieudane próby dostępu do plików, łamanie haseł, nadużycie uprawnień administracyjnych.

1.8.6 IMAP

Użytkownicy pobierają e-maile z serwerów przy użyciu protokołu IMAP (w przeciwieństwie, SMTP transferuje e-mail między serwerami). Hackerzy odkryli kilka błędów na wielu popularnych serwerach IMAP

1.8.7 IP spoofing

Jest wiele ataków, które wykorzystują możliwość fałszowania (lub "podszycia") adresu IP. Chociaż adres źródłowy jest wysyłany wraz z każdym pakietem IP, to nie jest faktycznie wykorzystywany do routingu. Oznacza to ,że intruz moze udawać ,że kiedy komunikuje się z serwerem. Intruz nigdy nie widzi pakietów odpowiedzi (chociaż komputer to robi, ale wyrzuca je daleko ponieważ nie dopasowuje do żadanego żądania jakie wysłałeś) Intruz nei może pobrać danych w ten sposób, ale może wysłać jeszcze komendy do serwera udawając ,że tak. IP spoofing jest często używany jako część innych ataków:

SMURF

Jeżeli adres źródłowy rozesłanego ping jest fałszywy, więc duża liczba komputerów odpowiada ofierze wskazaną tym adresem, przeciążając go (lub jego łącze)

Przewidywanie numeru sekwencji TCP

W uruchomionym połączeniu TCP, należy wybrać numer sekwencji na końcu,i serwer musi wybrać numer sekwencji na końcu. Starsze stosy TCP wybierają przewidywalne numery sekwencji, pozwalając intruzowi tworzyć połączenia TCP z fałszywym adresem IP (dla których nigdy nie zobaczy pakietu odpowiedzi) co pozwoli ominąć zabezpieczenia.

Zatrucie DNS przez przewidywalne sekwencje

Serwery DSN "rekurencyjnie" rozpoznają nazwy DNS. Zatem, serwer DNS, który spełnia żądanie klienta sam stanie się klientem kolejnego serwera w rekurencyjnym łańcuchu. Używane numery sekwencji są przewidywalne. W ten spoób intruz może wysłać żądanie do serwera DNS a odpowiedź z serwera utworzy z kolejnego serwera w łańcuchu. Wtedy uwierzy w sfałszowaną odpowiedź i używa tego do zaspokojenia innych klientów

1.8.8 Przepełnienie bufora

Niektóre ataki przepełnienia bufora to:

Przepełnienie DSN

Kiedy do serwera jest wysyłana zbyt długa nazwa DNS. Nazwy DNS są ograniczone do 6 bajtów na subkomponent lub 256 bajtów w sumie

Przepełnienia statd

Kiedy dostarczane sa zbyt długie nazwy plików

1.8.9 Ataki DNS

DNS jest podstawowym celem ponieważ jeśli możesz uszkodzić serwer DNS, możesz skorzystać z relacji zaufania

Zatruwanie bufora DNS

Każdy pakiet DNS zawiera sekcję "Question" i sekcję "Answer". Słabe serwery będą wierzyć (i buforować) Odpowiedzi, które wysyłasz z Questions. Wiekszość, ale nie wszystkie serwery DNS zostały poprawione w Listopadzie 1998 roku

1.9 Jakie są najczęstsze skanowania rozpoznawcze?

1.9.1 Wymiatanie ping

To proste skanowanie po prostu pinguje zakres adresów IP aby znaleźć jakiś aktywny komputer. Zauważ ,że większość zaawansowanych skanerów będzie używało innych protokołów (takich jak wymiatanie SNMP) do zrobienia tego samego.

1.9.2 Skanowanie TCP

Próby otwierania (nasłuchiwania) portów TCP szukając usług jakie może wykorzystać intruz. Skanowanie może używać zwykłych połączeń TCP lub niewidzialne skanowanie , które używa półotwartych połączeń (aby zapobiec ich logowaniu) lub skanowanie FIN (nigdy nie otwiera portów ,ale sprawdza czy ktoś nasłuchuje) Skanowanie może być sekwencyjne, losowe lub ze skonfigurowanej listy portów

1.9.3 Skanowanie UDP

To skanowanie jest trochę trudniejsze ponieważ UDP jest protokołem bezpołączeniowym. Technika ta wysyła śmieciowy pakiet UDP do żąanego portu. Większość komputerów odpowie komunikatem ICMP "Port docelowy nieosiągalny", wskazując ,że żadna usługa nie nasłuchuje na tym porcie. Jednak wiele komputerów tłamsi wiadomości ICMP, więc nie można tego zrobić bardzo szybko

1.9.4 Identyfikacja OS

Przez wysyłanie niepoprawnych (lub dziwnych) pakietów ICMP lub TCP, intruz może zidentyfikować system operacyjny. Standardy zwykle stanowią jak komputery powinny odpowiadać na poprawne pakiety, więc komputery wydają się zunifikowane w odpowiedzi na poprawne dane wejściowe. Jednak standardy (zwykle celowo) pomijają odpowiedzi na niepoprawne dane wejściowe. Zatem każdy system operacyjny unikalnie odpowiadają na

niepoprawne dane wejściowe w formie podpisu, tak że hackerzy mogą to wykorzystać dla wywiedzenia się o komputer docelowy. Ten rodzaj działalności występuje na niskim poziomie (np skanownie niewidzialne TCP), tak ,że nie zalogujesz się do systemów.

1.9.5 Skanowanie kont

Próby logowania do konta

- Konta bez haseł
- Konta z hasłem takim samym jak nazwa użytkownika, lub "password"
- Domyślne konta, które dostarczono z produktem (powszechny problem na SGI, czyni konfigurację łatwiejszą)
- Konta zainstalowane z oprogramowaniem produktu (popularne w Microsoft jak i w Unix'ie, spowodowane przez produkty, które uruchamiają swoje własne , specjalne konta użytkownika)
- Problemy anonimowych FTP (CWD ~root)
- Skanowanie portów rlogin/rsh/rexec, które mają wspierać zaufane logowania

1.9 Jakie są najczęstsze ataki DoS (Denial of Service?

1.10.1 Ping-of-Death

Wysyła niepoprawne fragmenty, które zaczynają się przed koncem pakietu, ale rozciąga poza koniec pakietu.

1.10.2 SYN Flood

Wysyłanie pakietów TCP SYN (które zaczynają połączenia) bardzo szybko, pozostawiając ofiary czekające na olbrzymią liczbę połączeń, powodując wyczerpywanie zasobów i opuszczanie właściwych połączeń. Nową obroną przeciwko temu są "SYN cookies". Każda strona połączenia ma swój własny numer sekwencji. W odpowiedzi na SYN, zaatakowana maszyna tworzy specjalny numer sekwencji, który jest "ciasteczkiem" połączenia potem zapomina o wszystkim co wie o połączeniu. Może ona potem odtworzyć zapomniane informacje na temat połączenia kiedy kolejny pakiet pochodzi z poprawnego połączenia

1.10.3 Land/Latierra

Wysyłanie sfałszowanego pakietu SYN z identycznym adresem/portem źródła / przeznaczenia, tak aby system przeszedł w nieskończoną pętlę próbując zakończyć połączenie TCP

1.10.4 WinNuke

Wysyła dane OOB / URG w połączeniu TCP na port 139 (Sesja NetBIOS / SMB), co powoduje zawieszenie Windows

1.1 Ile niebezpieczeństw niosą za sobą intruzi?

Często słyszę od ludzi stwierdzenie "Nie mam w systemie niczego co ktoś by chciał mieć". Przechodzę potem przez różne scenariusze , takie jak proste czy kiedykolwiek zapłaciła za coś w sieci kartą kredytową lub czy miał jakieś dokumenty finansowe lub z ubezpieczenia społecznego na własnym komputerze. Co ważniejsze, jest to kwestia odpowiedzialności prawnej. Jesteś potencjalnie odpowiedzialny za szkody spowodowane przez hackerów wykorzystujących twój komputer. Musisz być w stanie udowodnić przed sąem ,że podjąłeś "rozsądne" środki obrony przed hackerami. Na przykład rozważmy jeśli umieścimy urządzenie na szybkie łącze (modem kablowy lub DSL) i otworzyłeś konto administratora /root bez hasła. Wtedy jeśli hacker włamie się na tą maszyne, może użyć jej do włamania do banku, a wtedy możesz być pociągniety do odpowiedzialności, ponieważ nie podjąłeś najbardziej oczywistych środków zabezpieczenia komputera.

II ARCHITEKTURA

2.1 Jak wykrywać włamania?

2.1.1 Wykrywanie anomalii

Najpowszechniejszym sposobem ludzi na podejście do wykrywania sieciowych włamań jest wykrywanie statystycznych anomalii. Ideą tej metody jest pomiar stanów "podstawowych" takich jak statystyki wykorzystaniaCPU, aktywność dysku, logowania użytkowników, aktywność plików itd. Potem może zostać wyzwolony system ,kiedy pojawią się odchylenia od wskazań.Zaletą takiego podejścia jest to ,że można wykryć nieprawidłowości, bez konieczności zrozumienia tych nieprawidłowości. Na przykład powiedzmy ,że monitorujemy ruch na poszczególnych stacjach roboczych. System stwierdza ,że o 2 w nocy wiele z tych stacji zaczeło logowaćsię na serwery i realizowało jakieś zadania. To jest dość ciekawe i warto podjąć jakieś działania.

2.1.2 Rozpoznawanie podpisu

Większość komercyjnych produktów opartych o badanie ruchu, szuka dobrze znanych wzorców ataku. Oznacza to ,że dla każdej techniki hackerskiej,inżynierowie kodują coś do systemu przeciw tej technice. To może być tak proste jak dopasowanie wzorców. Klasycznym przykładem jest przkład każdego pakietu na kablu do wzorca "cgi-bin/phf?", który może wskazywać ,że ktoś próbuje się dostać do tego słabego skryptu CGI na serwerze WWW. Niektóre systemy IDS są zbudowane z dużych baz danych, które zawierają setki (lub tysiące) takich łańcuchów. Po prostu podpinają się pod przewód i wyzwalają przy każdym pakiecie, jeśli widzą ,że zawiera jeden z tych łańcuchów.

2.2 Jak NIDS dopasowuje podpisy przy ruchu przychodzącym?

Ruch składa sięz datagramów IP przepływających przez sieć. NIDS może przechwycić te pakiety jeśli przesyłane są kablem. NIDS składa się ze specjalnego stosu TCP/IP, który poniwnie składa datagramy IP i strumienie TCP. Wtedy stosuje poniższe techniki:

Weryfikacja stosu protokołu Liczba włamań, takich jak "Ping-Of-Death" i "TCP Stealth Scanning" używa naruszeń podstawowych protokołów IP, TCP, UDP i ICMP w celu zaatakowania komputera. Prosty system weryfikacji może osłabić niepoprawne pakiety. To może być ważne ,przy podejrzanym zachowaniu takim jak indywidualnie pofragmentowane pakiety IP.

Weryfikacja protokołu aplikacji Wiele włamań używa niepoprawnego zachowania protokołu, takiego jak "WinNuke", który stosuje nieprawidłowy protokół NetBIOS (dodając dane OOB) lub zatruwanie pamięci podręcznej DNS, któy ma ważny, ale nietypowy podpis. W celu skutecznego wykrywania takich włamań, NIDS musi reimplementować szeroki wybór protokołów warstwy aplikacji aby wykryć podjerzanych lub nieprwidłowe zachowania.

Tworzenie nowych logowalnych zdarzeń NIDS może być użyty do rozszerzenia możliwości audytowania oprogramowania zarządzającego siecią. Na przykład NIDS może rejestrować wszystkie protokoły warstwy aplikacji używane na komputerze. Systemy logowania zdarzeń (Zdarzenia WinNT, syslog Unix, SNMP TRAPS itp) mogą potem skorelować te rozszerzone zdarzenia z innymi zdarzeniami w sieci.

2.3 Co dzieje się po wykryciu ataku przez NIDS?

Rekonfiguracja firewalla

Konfigurujemy firewalla do filtrowania adresu IP intruza. Jednak, pozwala to jeszcze intruzowi zaatakować z innych adresów. Punkt kontrolny firewalla obsługuje "Suspicious Activity Monitoring Protocol SAMP" dla konfigurowania firewalli. Punkt kontrolny ma swój standard"OPSEC" dla rekonfiguracji firewalli dla blokowania sprawiających kłopoty adresów IP

dźwięk

Sygnał dźwiękowy lub odegranie pliku .WAV. Na przykład możesz usłyszeć nagrane "Jesteś atakowany"

SNMP Trap

Wysłanie datagramu SNMP Trap do konsoli zarządzania takiej jak HP OpenView, Tivoli, Cabletron Spectrum itp

Zdarzenia NT

Wysłanie zdarzenia do dziennika zdarzeń WinNT

syslog

Wysłanie zdarzenia do systemu zdarzeń syslog UNIX

wysłanie e-mail

Wysłanie maila do administratora powiadamiając o ataku

Logowanie ataku

Zapisanie informacji o ataku (znacznik czasowey, adres IP intruza, adres IP/ port ofiary, informacje o protokole

Zapisanie dowodów

Zapisanie trasy surowego pakietu dla późniejszej analizy

Uruchomienie programu

Uruchomienie oddzielnego programu do obsługi zdarzenia

Zakończenie sesji TCP

Utworzenie pakietu TCP FIN aby wymusić zakończenie połączenia

2.4 Jakie inne środki zaradcze istnieją oprócz IDS?

Firewalle

Większość ludzi myśli o firewallu jako pierwszej linii obrony. Oznacza to ,że jeśli intruz dowie się jak go ominąć (łatwe, zwłaszcza ,że wiekszość włamań jest dokonywanych przez pracowników za firewallem), będą musiekli rozejrzeć się po sieci. Lepszym sposobem jest myślenie o nim jako ostatniej linii obrony: powinieneś być pewien ,że komputry są prawidłowo skonfigurowane i działa system wykrywania intruzów, a następnie uruchomić firewall aby uniknąć script-kiddies. Zauważ ,że prawie każdy router obecnie może być skonfigurowany z pewnym filtrowaniem firewalla. Podczas gdy firewalle chronią przed dostępem z zewnątrz, pozostawiają sieć niechronioną przed intruzami wewnętrznymi. Oceniono ,że 80% strat z powodu "hackerów" ma miejsce przez ataki z wewnątrz.

Uwierzytelnianie

Powinieneś uruchomić skanery , które automatycznie będą znajdować otwarte konta. Należy egzekwować rygorystyczną politykę odnośnie haseł (minimum 7 znaków, wliczając w to liczby, znaki interpunkcyjne). Możesz również rozważyć pojedyncze podpisy na produktach i integrację tak wielu systemów haseł jak to możliwe, takich jak integracje RADIUS/TACACS UNIX lub NT (logowanie w tylu dial-up), integracje uwierzytelniania Unix i WinNT (z istniejącymi narzędziami takimi jak Kerberos w Windows 2000). Te systemy uwierzytelnienia pomoga również usuwać hasła "jawnym tekstem" z protokołów takich jak Telnet, FTP, IMAP, POP itp

VPN (Virtual Private Networks)

VPN tworzy bezpieczne połączenie przez Internet dla zdalnego dstępu (np dla telepracy). Przykład 1: Microsoft wykorzystuje technologię nazwaną PPPT (PPP przez TCP) wbudowaną w Windows. Nadaje to komputerowi dwa adresy IP, jeden dla Internetu, i jeden wirtualny dla sieci firmowej. Przykład 2: IPSec rozszerza tradycyjny protokół IP o bezpieczeństwo. Choć producenci VPN twierdzą ,że ich produkt VPN "poprawia bezpieczeństwo" w rzeczywistości jest to zmniejszenie bezpieczeństwa firmowego. Chociaż samo łącze jest bezpieczne (uwierzytelnianie ,szyfrowanie), oba końce łącza są szeroko otwarte. Komputery domowe zagrożone tylnymi dzrzwiami rootkit pozwalają hackerowi na osłabienie połączenia VPN, pozwala na pełną ,niewykrywalny dostęp do drugiej strony firewalla

Szyfrowanie

Szyfrowanie staje się coraz bardziej popularne. Możesz wybrać szyfrowanie poczty elektronicznej (PGP. SMIME), szyfrowanie plików (ponownie PGP) lub szyfrowanie systemu plików (BestCrypt, ponownie PGP)

Przynęty / pułapki

Programy, które pretendują do miana usług, ale które się nie reklamują. Może to być coś prostego jak jeden z wielu emulatorów BackOrifice (np NFR Back Orifice Friendly), lub tak złożone jak całe podsieci fałszywych systemów zainstalowanych do tego celu.

2.5 Gdzie mam umieścić systemy IDS w sieci?

Hosty sieciowe

Chociaż sieciowe systemy wykrywania włamań są tradycyjnie stosowane jako sondy, mogą być również umieszczone na hostach (w trybie nie -odbierania). Weźmy na przykład sieci komutowane gdzie pracownik jest na tym samym węźle komutacyjnym co dyrektor generalny, który uruchamia Win98. Komputery z Windows są całkowicie bezbronne i nie mają możliwości logowania, które mogłoby być wykorzystane do tradycyjnego systemu wykrywania włamań w sieci opartej o hosty. Pracownik może użyć sieciowego łamacza haseł na miesiąc, bez obawy ,że zostaną złapani. NIDS instalowany jako oprogramowanie do skanowania antywirusowego jest najwydajniejszym sposobem wykrywania takich włamań

obrzeża sieci

IDS jest najbardziej efektywny na obrzeżach sieci, takich jak obie strony firewalla, w pobliżu serwera dial-up i na łączach do sieci partnerskich. Łącza te mają tendencję do niskiej przepustowości (prędkości T1) takiej ,że IDS może nadążyć za ruchem.

Sieć szkieletowa WAN

Innym punktem o wysokiej wartości jest korporacyjna sieć szkieletowa WAN. Częstym probleme jest hackowanie z "peryferyjnych" obszarów do głównej sieci korporacyjnej. Ponieważ łącza WAN mają na ogół niską przepustowość, systemy IDS mogą nadążać.

Farmy serwerów

Serwery są często umieszczane w ramach własnej sieci, podłączone do switchy. Problem z tymi serwerami jest taki, że systemy IDS nie mogą nadążyć z ruchem o wysokim wolumenie. Na bardzo ważnych serwerach można zainstalować dedykowane systemy IDS, które monitorują tylko pojedyncze łącze serwera. Ponadto, serwery aplikacyjne mają skłonności do mniejsszego ruchu niż serwery plików, więc są lepszymi celami dla systemów IDS.

Sieci szkieletowe LAN

Systemy IDS są niepraktyczne dla sieci szkieletowych LAN, ze względu na ich wymagania wysokiego ruchu. Niektórzy sprzedawcy włączają wykrywanie IDS do switchy.. Pełny system IDS, który musi ponownie składać pakiety, jest mało prawdopodobne aby nadążał za ruchem. System skalowany, który wykrywa prostsze ataki ale może nadążyć jest lepszym wyborem.

2.6 Jak IDS pasuje do reszty mojego systemu bezpieczeństwa?

1. Umieść firewalle między obszarami sieci z różnymi wumaganiami bezpieczeństwa (tj Internet – sieć lokalna, użytkownik-serwer, firma – klienci itp).
2. Użyj skanera podatności sieci podwójnego sprawdzania firewalla i znajdź dziury jakie intruz może wykorzystać
3. Użyj skanerów zasad hosta aby upewnić się ,że są zgodne z przyjętymi praktykami (np najnowsze poprawki)
4. Użyj sieciowego systemu wykrywania włamań sieciowych i innych narzędzi z pakietu sniffowania, aby zobaczyć co się faktycznie dzieje
5. Użyj systemów wykrywania włamań opartych o hosty i skanery antywirusowe, aby oznaczyć skuteczne włamanie
6. Stwórz łatwe do naśladowania zasady, które jasną ustanowią odpowiedzi na włamanie

2.7 Jak można wykryć czy ktoś uruchomił NIDS?

NIDS jest zasadniczo snifferem, tak więc mogą być użyte standardowe techniki wykrywania snifferów. Przykładowo można zrobić traceroute wobec ofiary. To często generuje niskopoziomowe zdarzenia w IDS. Traceroute są nieszkodliwe i częste w sieci, więc nie wskazują na włamanie. Jednak ponieważ wiele ataków jest poprzedzonych traceroute, IDS i tak je będą zapiywać. W ramach systemu logowania, robimy odwrotne wyszukiwania DNS. Dlatego jeśli uruchomisz własny serwer DNS, możesz wykryć czy ktoś wykonuje odwrotne wyszukiwanie DNS na twoim adresie IP w odpowiedzi na traceroute.

III ZASADY

3.1 Jak zwiększyć wykrywanie włamań / profilaktykę w środowisku WinNT?

Poniżej mamy listę rzeczy, które sprawiają ,żę WinNT będzie bardziej bezpiecznym, wliczając w to wykrywanie jak również profilaktykę. Są one wylistowane w przybliżonej kolejności ważności.

1. Zainstaluj najnowszy service pack i "hot fixy". Jeśli używasz WinNT 4.0 i nie masz Service Pack 3 (SP3) zainstalowanego, intruz może włamać się do twojego systemu.
2. INSTALACJA: Użyj NTFS zamiast FAT. NTFS pozwala na uprawnienia do ustawienia per-file/ per-directory . NTFS pozwala również na kontrolowanie na podstawie per-file/pr-directory. Należy pamiętać ,że wiele osób zaleca używanie FAT jako dysku rozruchowego i NTFS dla wszytskich innych dysków (ze względu na łatwe wykorzystanie DOS'a przy naprawie błędów napędu FAT). Jednak użycie NTFS dla wszystkich dysków jest zdecydowanie bezpieczniejsze.
3. USRMGR. Zmień konto "Administrator". Popularnym atakiem jest użycie ataaku Słownikowego lub brute force na konto "administrator". Zwykłe konta mogą być skonfigurowane do automatycznego (i czasowego) "blokowania" po kilku nieudanyuch atakakch na konto. Jednak ta funkcja nie jest możliwa dla konta administratora, ponieważ pozwala na atak "odmowy usługi" (tj uniemożliwienie administracji komputera przez zablokowanie konta administratora)
4. USRMGR. Stwórz nowe konto nazwane "adminsitrator" dla wykrywania prób włamań.

5. USRMGR. Zablokuj konto "gość". Możesz również chcieć zmienić nazwę tego konta. Po zmianie nazwy konta "gość" możesz chcieć stworzyć nowe konto "gość" dla wykrywania prób włamań
6. NTFS. Wyłącz dostęp "zapis" dla "Każdego" w katalogu %systemroot%/system32
7. REGEDT32. Włącz kontrolę dla "HKEY_LOCAL_MACHINE\Security" aby wykryć zdalne przeglądanie rejetru.
8. INSTALACJA: Nie instaluj w katalogu "C:\WINNT". Czasami intruzi będą mogli mieć dostęp do pliku jeśli znają nazwę pliku; instalacja w innym katalogu zapobiega wiedzy a priori. Lepiej jeszcze zainstalować w C:\WINNT, potem przeinstalować do innego katalogu, potem włączyć kontrolę wewnątrz tego katalogu aby pojawiał sięalarm o ludziach chcących się dostać do tych starszych plików.
9. INSTALACJA: Użyj partycji rozruchowej tylko rozruchu i plików systemowych. Wstaw dane i apliakcje na oddzielnej partycji. Dobrym pomysłem jest oddzielenie apliakcji od danych.
10. PANEL STEROWANIA Włącz "Ochrona Hasłem" wygaszacza. Najlepszym wygaszaczem jest "Pusty Ekran". Sądzisz ,że wygaszacza uruchamia się w czasie jałowym, ale nie zawsze, więc możesz zwiększyć wydajność serwera przez użycie "Pustego Ekranu". To również redukuje moc pożeraną przez monitor, zwłaszcza te które mogą wykryć pusty ekran i same się wyłączają. W końcu, niektóre wygaszacze są podatne na włamania.
11. REGEDT32. Wyłącz automatyczne współdzielenie ADMIN&, C$, D$ itd poprzez parametr "AutoShare" w rejestrze. Parametr ten znajduje się w "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters" i jest to "AutoShareServer" dla WinNT Server lub "AutoShareWks" dla WinNT Workstation. Jest to DWORD, z wartością "1" dla włączenia (domyślne) lub wartością "0" dla wyłączenia. Będziesz musiał dodać wartość sam ponieważ nie istnieją już w rejestrze.
12. REGEDT32. Wyłącz informacje konta/współdzielenia przez konto anonimowe. Dodaj DWORD "RestrictAnonymous" z wartością "1" do klucza rejestru "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA".Zauważ,że jeśli widzisz błąd "Nie można odnaleźć kontrolera tej domeny", podczas ustawiania domeny zaufanych relacji, trzeba będzie zmienić te ustawienia z powrotem.
13. USRMGR. Jeśli używasz Domen (zmiast Stacji roboczych), zmień prawo użytkownika "Dostęp do tego komputera z sieci" na "Użytkownicy uwierzytelnieni" zamiast "Każdy". To wyłącza zdalny dostęp przez konta lokalne na komputerze i pozwala na dostęp przez konta domeny.
14. PASSPROP. Włącz blokadę konta "Administrator" dla dostępu zdalnego. Umożliwia to sytuację kiedy zdalny intruz nie odgadnie poprawnego hasła po trzech próbach. Po zablokowaniu administrator może się zalogować lokalnie w systemie konsolowym. Można również wyłączyć całkowicie dostęp zdalnego administratora w USRMGR przez usunięcie prawa "Dostęp do komputera z sieci" z "Administratorzy", ale to wyłącza całą zdalną administrację, co czyni administrowanie zbyt trudnym w dużym środowisku WinNT.

Rozważmy również zapobieganie fizycznym włamaniom do sieci. John Kozubik sugeruje użycie skryptów logowania dla wymuszenia ochrony hasłem wbudowanego wygaszacza .W skrypcie logowania umieśćmy taką linię:

```
regedit  /s  \\MY_PDC\netlogon\scrn.reg
```

A w pliku "scrn.reg" wstaw tekst:

```
REGEDIT4
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaveTimeOut"="1800"
"ScreenSaveActive"="1"
"SCRNSAVE.EXE"="c:\winnt\system32\logon.scr"
"ScreenSaverIsSecure"="1"
```

Spowoduje to zapytanie o hasło po 30 minuitach nieobecności użytkownika przed monitorem (nie loguje się, po prostu zmusza do ponownego podania hasła, zanim będziemy mieli ponowny dostęp)

3.2 Jak zwiększyć wykrywanie włamań / profilaktykę w środowisku UNIX?

1. Nie instaluj więcej usług niż potrzebujesz.
2. Używaj "netstat" lub skanera TCP/UDPi "rpcinfo" dla wylistowania wszystkich usług na komputerze. Ponownie zastanów się czy wszystko dobrze zrozumiałeś zanim wyłączysz

Oczywiście możesz chcieć rozważyć aktualizację systemu.

3.3 Jak zwiększyć wykrywanie włamań / profilaktykę w środowisku Macintosh?

Macintosh'e są systemami "użytkownika końcowego", i obsługują kilka usług, które mogą być zhackowane. Dla porównania komputerów z Windows jest więcej, a komputery UNIX mają wiele interesujących (hackowalnych) usuług uruchomionych. Tak więc Macintoshe nie są częstym celem itruzów. Poza tym nie ma nic szczególnego.

3.4 Jak zwiększyć wykrywanie włamań / profilaktykę w przedsiębiorstwie?

Pierwsze i najważniejsze, stworzyć zasady bezpieczeństwa. Powiedzmy ,że przeglądasz sieć późnymwieczorem i widzisz itruza w toku działania.Co robisz? Czy pozwolić na włamanie i zbierać dowody? Odłączyć wtyczkę? Jeśli tak to można wyjąć wtyczkę w firewallu między wewnętrzną a zewnętrzną siecią. Czy może zablokować uzytkownikom dostęp do twojej strony WWW)? Kto ma upoważnienia do wyjęcia wtyczki? Priorytety muszą być ustawione na swoim miejscu przez CEO korporacji. Rozważmy scenariusz w którym myślisz ,że zostałeś zaatakowany,więc wyciągasz wtyczkę. Użytkownicy są niezadowoleni. Ale okazało się ,że myliłeś się, więc jesteś ugotowany. Nawet kiedy gdy dzieją się rażące ataki, kilka osób może wyjąć wtyczkę z obawy przed takimi reperkusjami. Kradzieże danych są teoretyczne a wkurzeni użytkowncy bardzo realni. Dlatego potrzebujesz zasad z samej góy, które jasno stanowią o najważniejszych rzeczach i jasno opisuje procedury, co sięma dziać kiedy istnieje podejrzenie włamania.

3.5 Jak należy wdrażać system wykrywania włamań w przedsiębiorstwie?

Pomyśl o tym jak można skonfigurować poniższe systemy aby wykrywać intruzów:

1. System Operacyjny taki jak WinNT i Unix pochodzą z zintegrowanymi funkcjami logowania / audytowania , które mogą być wykorzystywane do monitorowania krytycznych zasobów bezpieczeństwa.
2. Usługi, takie jak serwery WWW, serwery e-mail i bazy danych również zawierają funkcję logowania / audytowania. Dodatkowo, jest wiele narzędzi, które mogą być użyte do parsowania tych plików aby wykryć podpisy włamań
3. System Wykrywania Włamań Sieciowych, który obserwuje ruch sieciowy próbując odkryć próby włamań.
4. Firewalle zazwyczaj mają możliwości wykrywania włamań sieciowych. Po tym wszystkim, blokowanie włamań jest ich głównym celem; byłoby głupotą również nie wykrywanie włamań
5. Platformy zarządzania siecią (takie jak OpenView) mają narzędzia pomocne administratorom sieci ustawiać alarmy pdo kątem podejrzanych działań. Wszystkie urządzenia SNMP powinny wysyłać pułapkę "Błąd Uwierzytelniania" a konsole zarządzania

powinny alarmować administratorów kiedy to zniknie.

3.5 Co powinienem zrobić kiedy zostałem zhackowany?

Przeczytaj checklistę wykrywania włamań CERT pod ftp://ftp.cert.org/pub/tech_tips/intruder_detection_checklist
W przeważajacej części, dobra odpowiedź wymaga abys ustawił dobrą defensywną taktykę na pierwszym miejscu. Zawiera ona:

zespół reagowania na incydenty

Ustaw "zespół reagowania na incydenty". Określ ludzi którzy powinni zostać wezwani, kiedy jest podejrzenie o włamanie w toku. Zespół ten musi być "międzyresortowy" i powinien mieć takich ludzi jak :

wyższe kierownictwo

Należy określić kogoś , kto ma uprawnienia do obsługi eskalacji problemów. Na przykład jeśli firma ma usługi nandlu online, należy znaleźć kogoś kto ma prawo "wyciągnąć wtyczkę"

HR (Zasoby ludzkie)

Wiele ataków pochodzi od wewnętrznych pracowników. Składa się zarówno z poważnych ataków (crackowanie komputerów) jak również ataków uciążliwych takich jak niewłaściwe przeglądanie serwerów plików dla wyszukania listy klientów, która może być potem otwarta

personel techniczny

Bezpieczeństwo jest często odrębne od zwykłej działalności MIS. Jeśli wykryto próbę ataku na systme, musisz wiedzieć do kogo w MIS możesz się zgłosić

osoby z zewnątrz

Identyfikacja osób spoza firmy, z jakimi możesz się skontaktować. To może być lokalny ISP (na przykład pomoc przy atakach SMURF), lokalna policja/ To nie muszą być kniecznie "formalni" członkowie zespołu bezpieczeństwa.

Zespół bezpieczeństwa

Oczywiście najważniejszymi w zespole będą ludzie którzy sami zajmują się bezpieczeństwem. Należy pamiętać, że "członkowie zespołu" muszą być dołączeni do każdego zdarzenia. Na przykład, możesz zwrócić się do wyższej kadry w sprawie poważnych ataków. Może nie będą wzywani bezpośrednio, ale muszą być poinformowani aby móc podjąć odpowiednie decyzje.

Procedura odpowiedzi

Wytyczne co do podjęcia działań. Na przykład, musisz zdecydować jakie są twoje priorytety między czasem działania sieci a włamaniem: możesz wyciągnąć wtyczkę z sieci za każdym razem kiedy podejrzewasz włamanie? Czy chcesz pozwolić na kontynuowanie włamania aby zebrać więcej dowodów? Postanów teraz, i uzyskaj zgodę CEO , bo podczas ataku nie będzie na to czasu.

Linie komunikacyjne

Wytyczne co do komunikacji. Czy rozszerzasz informację w przedsiębiorstwie w łańcuchu od swojego szefa do CEO czy poziomo do innych jednostek? Czy bierzesz udział w organizacji zgłaszających incydenty? Czy informujesz policję? Czy informujesz partnerów (dostawców / klientów) , którzy są podłączeni do sieci (która może być zagrożona lub od

kogo pochodzi atak)? Czy ukrywasz włamania przed prasą?

Porcedury logowania

Skonfiguruj procedury rejestrowania / audytu / monitorowania; pierwsze o czym najczęściej się myśli po ataku ,jest to jak udało im się zalogować, aby dowiedzieć się co się stało.

Szkolenia / próba

Prowadzenie we wszystkich tych kwestiach. Każa osoba zainteresowana musi zrozumieć zakres tego co musi zrobić. Załóżmy, ogromną penetrację sieci przez hackera. Większość penetracji hackera zakończyły się powodzeniem ponieważ praktycy firmowi nie byli przygotowania na ich ataki.

Ponieważ sieci komputerowe rosną bardzo szybko, nie ma wystarczającej liczby przeszkolonych osób do obsługi włamań. Podobnie sieci rosnące metodą ad hoc, więc i logowanie / audytowanie jest przypadkowe. Takie warunki prowadzą do stanu ,że ludzie nie wiedzą co robić kiedy zostaną zaatakowani, a ich sieci nie są wystarczająco stabilne.

3.6 Jak należy reagować , gdy ktoś mówi mi,że został zhackowany z mojej strony?

Na liście dyskusyjnej IDS, ktoś zapytał jak powinien odpowiedzieć jak odpowiedzieć na taki e-mail:

```
Poniżej znajduje się logowanie do połączenia telnet z komputera w
waszej domenie. Podłączony komputer nie oferuje publicznie takiej
usługi, więc można założyć ,że jest to próba wybadania przestrzeni
IP dla słabszych komputerów. Traktujemy tę sprawę bardzo poważnie,
i mamy nadzieję,że Państwo również. Prosimy podjąć działania w tej
sprawie i proszę odpowiedzieć na ten adres jakie działania Państwo
podjęli.
6 listopada 07:13:13 pbreton in.telnetd [31565]: odmowa połączenia
z xx.xx.xx.xx
```

Ten wpis został prawdopodobnie wygenerowany przez tcpwrappers, funkcja która poprawia logowanie i kontrolę dostępu do usług w UNIX. Pokazuje to nieautoryzowane próby z twojej strony do określonego komputera. Jak stwierdzono w wiadomości e-mail,może to być automatyczne przeszukanie jakiegoś rodzaju. Najpopularniejsze protokoły przeszukiwania to ICMP, FtP, SMTP, NNTP i Telnet. W każdym razie, jest to próba sondy, nie ataku. Ponadto, nie ma innych dowodów potwierdzających. Jak zauważył Greg Drew może być wiele łagodnych powodów:

- Ktoś wpisał "telnet xx.xx.xx.xx" i źle wpisał adres IP
- Ktoś chciał wpisać "telnet xx.xx.xx.xx 25" do połączenia z usługą STMP w odpowiedzi odbierając spam ze strony. Osoba ta może zapomniała o "25" lub źle wpisanym "23"
- Ktoś chciał zrobić szerokie skanowanie na komputerach docelowych w odpowiedzi na spam.
- Mogło to być pomyłką (ktoś miał tam konto na tym komputerze ,ale już nie ma)

Ale jest też wiele niecnych możliwości:

- Witryna została już zhackowana,a hacker prowadzi skanowanie z zainfekowanego komputera
- Jeden z pracowników używa tego komputera do hackowania

Może to też być atak typu inżynieria społeczna. Komunikat z pytaniem (poleceniem) do kontaktu z nimi dla opisania działań jakie musisz podjąć. Jeśli t ozrobisz, opowie ci to wiele o sieci:

- Cel ma poprawny adres IP (choć nie na tyle interesujący)
- Twój adres IP (powyższy komunikat prawdopodobnie wysłany do "postmastera" lub dobrze znanego adresu, ale prawdopodobnie odpowiesz z własnego adresu
- Twój poziom gotowości: jeśli wróciś z kiepską odpowiedzią (taką jak "nie możemy podjąć działań, bo nie mamy dzienników logowania"), wiedzą ,że twoja sieć jest podstawowym terytorium hackowania.
- Może to być "spam inżynierii społecznej". Nadawcą komunikatu może być firma szukajaca nabywców na produkty wykrywania włamań.

Jak się okazało, incydent był łagodny. Odbyła się rekonfiguracja sieci docelowej i "nieautoryzowany" użytkownik nie wiedział o tym, i był nieprawidłowo zalogowany.

3.7 Jak zebrać wystarczającą ilość dowodów na temat hackera?
Ciekawym polem działania IDS jest zbieranie informacji o incydencie i identyfikacji hackera. Może być to trudne, ponieważ elita hackerska będzie przeprowadzać swoje ataki z innych zhackowanych systemów. Hackerzy równie często wykorzystują adres IP spoofing, który może pojawiać się jako atak z komputerów, które nawet nie są włączone. Najlepszą techniką jest zebranie jak najwięcej informacji jak się da. Na przykład, umieściłem sniffer pakietów do przechwytywania tracefile na naszej lini T-1 zapisując plioki na 16 gigowym dysku twardym.

IV. PRODUKTY

Ta sekcja omawia różne główne produkty sieciowego IDS

4.1 Jakie są dostępne darmowe / płatne systemy wykrywania włamań?
Najbardziej kompletną listą dysponuje COAST Intrusion Detection System Resources , na stronie http://www.cs.purdue.edu/coast/ids

4.2 Jakie są dostępne komercyjne systemy wykrywania włamań?
Nowości mogą być znalezione na http://www.nwc.com/1023/1023f19.html
Należy zakładać ,że częśćz tych danych może stać się nieaktualne ,z powodu tego ,że informatyka bardzo szybko się rozwija.

4.2.0 BlackICE
BlackICE ma wiele wersji. Jądro jest zbudowane wokół "BlackICE Sentry", pełny system wykrywania włamań sieciowych. Są również wersje hostowe/hybrydowe. Które uruchamiają się na pulpicie Windows z wbudowanym osobistym firewallem. Cechy wyróżniające BlackICE Sentry to:

- Pełna, 7 warstwowy , stabilny analiza protokołów
- Technika anty-uchylania
- Wyjątkowo szybka, łatwa obsługa pełnego 100 Mbps pasma

4.2.1 CyberCop Monitor
CyberCop Monitor jest hybrydowym host/sieć IDS'em, który analizuje ruch w sieci od i do hosta jak również EventLog Windows NT i działania uwierzytelniania Windows NT

- Opracowany interfejs użytkownika pod Microsoft Management Console, zarówno zintegrowane CyberCop Monitor i SMI Console dostarcza łatwego do użycia interfejsu graficznego dla lokalnego/zdalnego raportowania, i zdalnej instalacji.
- Edytor konfiguracji pozwala na własne ustawienia i progi dla każdego środowiska, wliczając w to profile bezpieczeństwa, grupy kont, czas i podsieci

- Rozbudowane filtrowanie używające zasad filtorwania dla każego podpisu
- Funkcja raportowania kalescencyjnego hamuje denial of service na samym IDS
- Scalone raportowanie w zakresie monitorowania i skanowania informacji na system w opcją analizy, wliczając w to wykresy 3D i wykresy z bazy danych SQL

4.2.2 RealSecure
Internet Security Systems jest pierwszą i jedyną firmą, która powiązała zarówno wykrywanie włamań (ISS RealSecure) i wykrywanie podatności (ISS Internet Scanner) w zintegrowaną platformę bezpieczeństwa dla orgranizacji, aby pomóc zaplanować, analizować i zarządzać bezpieczeństwem w sposób ciągły. ISS RealSecure jest składnikiem rodziny produktów ISS SAFEsuite, które obejmuje zarządzanie ryzykiem bezpieczeństwa w całej firmie. ISS RaelSecure jest liderem na rynku Wykrywania Włamań z zintegrowanymi rozwiązaniamio dla hosta i sieci. ISS RealSecure zawiera ponad 400 podpisów ataków z możliwością dla klientów,zarówno w sieci i na hoście, rozwiązania dla dodawania lub modyfikacji ich własnych podpisów.

4.2.3 NetRanger
Pierwotnie produkt Wheelgroup, kupiony przez Cisco.

4.2.4 eTrust Intrusion Detection
Dawniej Memco/Abirnet/PLATINIUM SessionWall, obecnie właśność Computer Associates, wprowadzony do obrotu jako eTrust Intrusion Detection. Pierwotnie SessionWall zaczynało pd firewalla/ platformy inspekcji treści, które wtrącił w strumień ruchu.

4.2.5 NFR
NFR jest dostępny w wielu postaciach: wersja darmowa, "NFR Intrusion Detection Appliance", z bootowalnej płyty CD, i paczki u trzech sprzedawców , którzy dodali do niego swoje własne funkcje. Jedną z popularnych funkcji NFR jest "N-code", w pełni funkcjonalny język programownia, zoptymalizowany pod kątem możliwości wykrywania włamań. Mają pełno parsowanie SMTP napisany w N-code.

4.3 Co to jest system "network grep"?
System "network grep" jest oparty o przechwytyywanie surowych pakietów pompowanych przez parser "wyrażeń regularnych", który znajduje wzorce w ruchu sieciowym. Przykładem wzorca będzie :"/cgi=bin/phf", który wskazywałby próbę wykorzystania wrażliwego skryptu CGI nazwnaego "phf". Po zbudowaniu takiego systemu, analizujemy dobrze znane ataki, wekstrahując określone łańcuchy charakteryzujące te ataki, a potem dodanie ich do bazy danych wzorców. "Regexp" (wyrażenia regularne) jest wspólnym porównywaniem wzorców językowych w środowisku Unix. Podczas gdy tradycyjnie jest wykorzystywane do przeszukwiania plików tekstowych, może być również użyte do dowolnych danych binarnych. W rezczywistości, takie systemy mają bardziej elastycznne kryteria dopasowania, jak znajdowanie portów czy dopasowanie flag TCP.
"libpcap" (biblioteka do przechwytywania pakietów) jest wspólną biblioteką dostępną dla systemów Unix, która "sniffuje" pakiety w przewodzie. Większość systemów wykrywania włamań opartych na Unix(jakiegokolwiek rodzaju) używa libpcap, chociaż wiele z nich optymalizuje sterowniki dla małego podzbioru platform. Kod źródłowy obu modułów jest ogólnie dostępny. Duża liczba systemów wykrywania włamań przekazuje wyjście z libpcap (lub tcpdump) do parsera wyrażeń regularnych, gdzie wyrażenia pochodzą z pliku na dysku. Niektóre z prostszych systemów nawet nie używają wyrażeń regularnych i po prostu porównują pakiety ze znanymi wzorcami bajtów. Jeśli chcesz budować taki sam system, poczytaj o "tcpdump" i wyrażeniach regularnych. Ta klasa systmów wykrywania włamań ma jedą zaletę: jest najłatwiejsza do aktualizacji. Produkty tej klasy konsekwentnie będą miały największą liczbę "podpisów" i będą najszybsze na rynku w wykrywaniu nowych ataków "skryptowych". Jednakże podczas gdy takie systemy mogą mieć

największą liczbę "podpisów", wykrywają mniejszą liczbę "poważnych" włamań. Na przykład 8 bajtów "CE63D1D216E713CF" kiedy są widoczne na początku danych UDP wskazują ruch BackOrifice z domyślnym hasłem. Mimo ,że 80% ataków BackOrifice używa hasła domyślnego, pozostałe 20% korzysta z różnych haseł i nie będzie wykryte przez system. Na przykład zmaina hasła BackOrifice do "obejści" zmieni wzór na "8E42A52C 0666BC4A" i zostanie niezauważone przez systemy "network grep". Niektóre z tych systemów nie łączą ponownie datagramów IP lub strumieni TCP. I znowu hacker może po prostu zmienić konfigurację rozmiaru MTU na komputerze aby ominąć systemy regexp-pcap. W powyższym przykładzie, 64 bitowy wzorzec nie jest tak rzadki, że nie byłby widoczny w ruchu. Spowoduje to wywołanie alrmu , nawet kiedy BackOrifice nie jest obecny. Systemy oparte na analizie protokołu nie mają takich problemów. Łapią wszystkie wystąpienia ataków a nie tlko popularne odmiany; wynika z tego mniejsza liczba fałszywych alarmów; i są one w stanie działaćszybciej pnieważ dekodowanie protokołu nie musi "szukać" ramki. Są one w stanie dokładniej zdiagnozować problem, na przykład rozróżnić między "Back Orifice PING)" (który jest nieszkodliwy, a "Back Orifice kompromis" (występujący w warunkach ekstremalnych). Z drugiej strony, często podejmuja tygodniowe dodawanie nowych sygnatur analizy protokołów (zmiast godzinnych) ze względu na konstrukcję i testowanie stron. Ponadto nadmiernir agresywne próby ograniczania fałszywych alarmów również prowadzą do brakku rzeczywistych ataków w niektórych przypadkach. Jednak takie systemy mają przewaga nad systemami analizy protokołów. Ponieważ nie mają zapisane jak ruchsieciowy wygląda, mogą często wykrywać ataki, które przepuszczają inne systemy. Na przykład, jeśli firma uruchomi serwer POP3 na innym porcie, prawdopodobne jest ,że systemy analizy protokołów nie wykryją tegop. Z drugiej strony styl network-grep niekoniecznie dba o numery portów i sprawdzi same podpisy niezależnie od portów.

4.3.1 Bro

System wykrywania włamańVern Paxon's Bro . Vern Paxon napisał wiekszą część libpcap, na której opiera się wiele innych systmów wykrywania włamań (jak NFR czy Dragon)

4.3.2 Snort

Snort ostatni stał się bardzo popularny i uważany jest za naprawdę fanje narzędzie przez wiele osób. Zawiera ponad 100 własnych sygnatur, a inne można znaleźć w Internecie. Poniżej mamy przykładową regułę:

```
# tu mamy przykład wykrycia ataku Phf ,w którym jest poszukiwany
# prosty ciąg tekstowy w warstwie aplikacji
alert tcp any any -> 192.168.1.0/24 80 (msg:"PHF attempt";
content:"/cgi-bin/phf";)
```

Mówi o alarmie połączenia TCP z dowolnego adresu IP i dowolnego portu do 192.168.1.x podsieci portu 80. Wyszukuje zawartość "/cgi-bin/phf" gdziekolwiek w treści. Jeśli znajdzie taką zawartość, będzie alarmował konsome komunikatem "Próba PHF"

Korzystanie ze snort jest zwykle wykonywane w następujący sposób:

- Filtry BPF (część libpcap)są konfigurowane do zmniejszania nacisku na pewien typ ruchu
- Podejmowana jest decyzja co do tego, któe adresy IP są wewnętrzne a które zewnętrzne dla dalszego zawężania
- Edytowane są zasady w celu dopasowania do lokalnego środowiska
- Uruchamia się system
- Zasady są dalej edytowane dla usunięcia fałszywych alarmów

Ponadto snort ma wiele opcji używanych do wykrywania ruchu w sieci.

4.3.3 Argus
Argus sam nie jest systemem wykrywania włamań. Jednak monitoruje pakiety w przewodzie i generuje zdarzenia logowania. Możesz potem przetwarzać te wpisy dla znajdowania włamań.

4.4 Jakich narzędzi używają intruzi aby włamywać się do systemów?

4.4.1 Narzędzia UNIX
Narzędzia te pochodza albo z platformy UNIX albo mogą być ściągnięte za darmow

ping
: sprawdza czy host jest aktywny

traceroute
: znajdowanie drogi do hosta

nslookup/dig
: odkrywanie wszystkich informacji DNS

whois
: dowiadywanie się o wewnętrznych informacjach rejestracji

finger
: dowiadywanie się kto jest zalogowany i informacja o użytkownikach

rpcinfo
: dowiadywanie się jakie usługi RPC są uruchomione

showmount
: wyświetlanie akcji na komputerze

SAMBA
: wyświetla info o WinNT SMB

telnet
: najstarszy z nich – pozwala ci się połączyć i pogrywać z dowolonym protokołem tekstowym (HTTP, FTP, SMTP itp)

4.4.2 Narzędzia WinNT
Wszystkie narzędzia UNIX mogą być zastosowane z WinNT. Jest również kilka dla WinNT

nbtstat
: odkrywa informacje NetBIOS o zdalnej maszynie

net view
: jest to program LANMAN, który pozwala zdalnie podglądać akcje WinNT

4.4.3 Określone narzędzia hackera
Standardowy zestaw narzędzi dla intruza:

netcat
: charakteryzowany jako "Szawajcarski Nóż Wojskowy TCP/IP", pozwala intruzowi na interakcję z protokołami skryptowymi, zwłaszcza z protokołami tekstowymi

crack/NTcrack/L0phtCrack/ itp
: które łamią hasła sieciowe (Słownikowo lub Brute Force). Te pakiety również zaweirają narzędzia do zrzucania haseł do bazy danych i sniffowanie ich na kablu.

Narzędzia sniffowania
: dla oglądania surowego ruchu w sieci, takie jak Gobbler, tcpdump a nawet Network Associates Sniffer Network Analyzer

Skanery portów TCP i UDP
: dla skanowania / strobowania / próbkowania portów TCP jakie mogą być dostępne. Skanery

portów TCP mogą być również uruchamiane w trybie niewidzialnym dla uniknięcia logowania

Pirn sweeper

dla pingowania dużej liczby komputerów aby zobaczyć które są aktywne

Paczki exploitów

które są ustawiane na jeden lub więcej programów, które wiedzą jak wykorzystać dziury w systemie

Audytorzy bezpieczeństwa zdalnego

tacy jak SATAN, który wyszukuje dobrze znane dziury w komputerach w całej sieci

War dialer

który wybiera wiele numerów telefonów szukając portów dial-up

NAT

jest oparty na kdzie SAMBA, i jest użyteczny dla odkrywania informacji NetBIOS/SMB z serwerów Windows i SAMBA

Skanery

wszystkie programy (jak SATAN, ISS, CyberCop Scanner), które sondują system pod kątem słabości. Sprawdzają ogromną liczbę luk i są na ogół zautomatyzowane, dzięki czemu hacker ma najwyższą stopę zwrotu przy minimalnym wysiłku

4.5 Jakich innych narzędzi freeware/sharware do wykrywania włamań powinienem być świadomy?

4.5.0 NFR, Research version

"NFR Research Version" jest konfiurowalnym zbiorem narzędzi, dostępnym w Internecie do badań i niekomercyjnego zastosowania. Jest to oprogramowanie "as is", które wymaga wiedzy od użytkownika do instalacji i konfiguacji. To nie jest system wykrywania włamań "plug and play".

4.5.1 tcpwrappers

Tcpwrappers jest dodatkiem do systemów UNIX i umieszczony jest między inetd a usługami (takimi jak FTP, telnet) . inetd najpierw będzie wywoływał tcpwrappers, który zrobi kilka uwierzytelnienień (przez adres IP) i logowanie. Potem tcpwrappers wywoła rzeczywistą usługę , w razie potrzeby.

4.5.2 IDS dla Checkpoint Firewalls

Analiza wpisów dziennika firewalli jest bardzo podobna do analizy sieciowej.

4.5.3 Shadow

Myślę ,że jest to projekt używany w Marynarce Wojennej do śledzenia włamań i generowania raportów na ich temat.

4.5.4 AAFID

COAST Purde to rozproszony agent.

4.5 Czy są dostępne NIDS dla mojego hosta?

Nowa klasa NIDS uruchamianych na hostach w trybie nie – odbiorczym

4.5.1 Network ICE / BlackICE Defender

Pierwszy taki system BlackICE Defender firmy Networ IDE wydano w połowie 1999 roku. System zawiera także osobisty firewall. Skierowany jest do węzłów końcowych i serwerów

4.5.2 Network Associates / CyberCop Monitor

Drugi system to CCM z Network Associates, wydany pod koniec 1999 roku. Przede wszystkim używany jako "IDS oparty o host", większość włamań wykrywane jest w sieci.

4.5.3 CybeSafe / Centrax NNID

W lutym 2000 roku, CyberSafe zaanonsował swój "węzeł wykrywania włamań sieciowych (NNID)". Wydaje się ,że wersje swoich NIDS Centrax są na licencji odbierania i nie – odbierania począwszy od wersji 2.3.

4.5.4 ISS / RealSecure Micro-Agent

ISS ogłosił wersję "Micro-Agent" RealSecure NIDS.Wskazuje ,że zawierać będzie funkcje "blokowania", które będą się składać z jakiegoś rodzaju firewalla.

V. ZASOBY

5.1 Gdzie mogę znaleźć aktualizacje na temat nowych luk w zabezpieczeniach?

5.1.1 CERT (Computer Emergency Response Team)

Jeśli jest jakiś problem z bezpieczeństwem, może ewentualnie zajrzeć do doradztwa CERT. CERT (Computer Emergency Response Team) został utrworzony przez wiele uniwersytetów i DARPA w odpowiedzi na Morris Worm z 1988 roku

5.1.2 AUSERT (Australian Computer Emergency Response Team)

http://www.auscert.org.au

5.1.3 CIAC (Computer Incident Advisory Capability) Departamentu Energii USA

5.2 Jakie są inne środki bezpieczeństwa i wykrywania włamań?

5.2.1 Archiwum COAST Purdue

Najlepsza strona w sieci do nauki o IDS i bezpieczeństwie ogólnie. Zobacz http://www.cs.purdue.edu/coast, http://www.cs.purdue.edu/coast/intrusion-detection i http://www.cs.purdue.edu/coast/ids

5.2.2 Instytut SANS

Myślę ,że może być to najlepsza strona z informacjami o bezpieczeństwie dla osób, które same nie są hackerami. Docelowymi odbiorcami są specjaliści MIS, którzy zajmują się obroną swoich sieci. http://www.sans.org/

5.2.3 L0pht Heavy Industries

Kilku hackerów, tworzących bardzo dobre narzędzia i użyeczne alerty ukierunkowane na Windows.

5.2.4 Technical Incursion Countermeasures

Lubię tę stronę; ma kilka dobrze zorganizowanych informacji na temat włamań (wtargnięć) http://www.ticm.com/

5.2.5 Strona Michaela Sobireya IDS
http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html

5.2.6 Baza danych advICE
http://www.networkice.com/advice/Countermeasures/Intrusion_Detection/default.htm

5.3 Jakie są strony, które są ciekawe?
Strony te agregują informacje na temat innych stron. Warto tam zajrzeć

5.3.1 Strona o bezpieczeństwie NIH
http://www.alw.nih.gov/Security/

5.3.2 NTSecurity.net
http://www.ntsecurity.net/

VI. IDS i Firewall

6.1 Dlaczego muszę mieć IDS jeśli już mam firewall?
Wielkim nieporozumieniem jest to ,że firewall rozpoznaje ataki i blokuje je. To nie prawda.
Firewalle są po prostu urządzeniami, które wyłącza wszystko, potem włącza tylko kilka dobrze sobie znanych pozycji. W idealnym świecie, system byłby już "zablokowany" i bezpieczny a firewalle byłyby niepotrzebne. Korzystamy z firewalli ponieważ luki w zabezpieczeniach są otwierane przypadkowo. Tak więc podczas instalacji, pierwsza rzecz jakąrobimy to zatrzymanie CAŁEJ komunikacji. Administrator firewalla potem ostrożnie dodaje "zasady", które pozwalają określić typ ruchu przechodzącego przez firewall. Na przykład, typowy firewall korporacyjny umożliwia dostęp do Internetu , zatrzyma cały ruch datagramów UDP i ICMP, zatrzyma połączenia TCP, ale pozwoli na połączenia wychodzące TCP. Zatrzymuje to wszystkie połączenia przychodzące od hackerów Internetowych, ale nadal pozwala użytkownikom wewnętrznym na połączeniu w kierunku wychodzącym. Firewall jest po prostu ogrodzeniem wokół sieci, z kilku dobrze dobranymi bramami. Ogrodzenie nie ma możliwości wykrywania prób włamania (takich jak kopanie dziury pod nim). Po prostu ogranicza dostęp do wyznaczonych punktów. Podsumowując. Firewall nie jest dynamicznym systemem obrony, jak sobie wyobrażą użytkownicy. W przeciwieństwie IDS jest dużo bardziej niż dynamicznym systemem. IDS rozpoznaje ataki przeciwko sieci, któych nie widzi firewall. Na przykład, w kwietniu 1999 roku, wiele stron zostało zhckowanych przez błąd ColdFusion. Strony te wszystkie miały firewalle, które ograniczały dostęp tylko do serwera na porcie 80. Jednak, serwer WWW został zhackowany. Tak więc, firewall nie obronił ich. Z drugiej strony, system wykrywania włamań dostrzegłby atak, ponieważ pasuje do wzorca podpisu skonfigurowanego w systemie. Kolejny problem z firewallami jest taki ,że są one na granicy sieci. Około 80% wszystkich strat finansowych z powodu włamań pochodzi w wnętrza sieci. Firewall na obrzeżach sieci nie widzi niczego co dzieje się wewnątrz, ale widzi tylko ruch, który przewchodzi między siecią wewnętrzną a Internetem.
Powody dla których trzeba dodać IDS do firewalla:

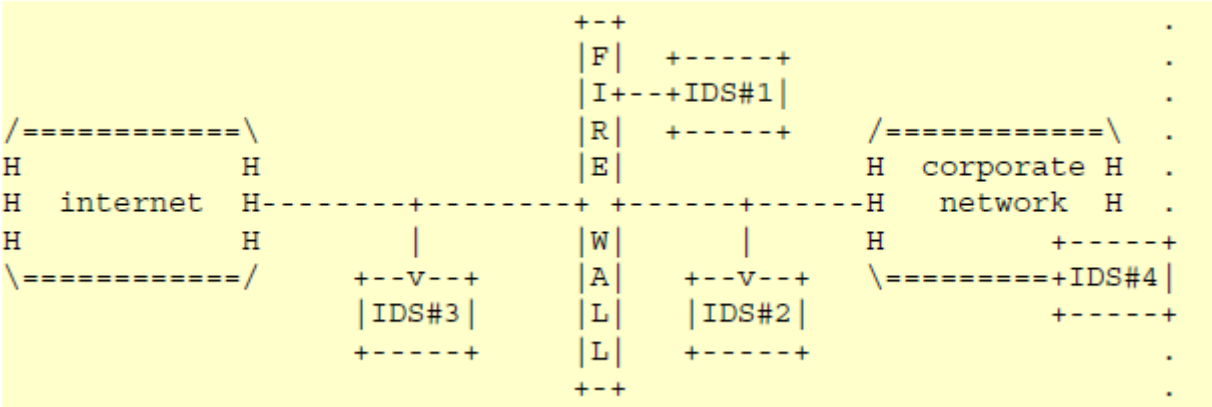
- Dwukrotne sprawdzenie źle skonfigurowanego firewalla
- Przechwytywanie ataków, które firewall uprawomocnia (np ataki na srwery WWW)
- Przechwytywanie nieudanych prób
- Przechwytywanie wewnętrznego hackera

"Głęboka obrona i przesadna paranoją są twoimi przyjaciółmi" (Bennett Todd) Hackerzy są dużo zdolniejsi niż myślisz; tym bardziej obrona musi być lepsza. A dalej nie chroni cię przed zdeterminowanym hackerem. Podniesie to im jednak poprzeczkę co do wymagań.

6.2 Jak to jest ,że hackerzy przechodzą przez firewalle?
Większość administratorów ma konserwatywne podejście, Łatwo jest zbudować firewall , który nie będzie zhackowany będąc zbyt konserwatywnym i paranoikiem, i po prostu wyłączyć wszystkie niezbędne usługi. Jednak w świecie rzeczywistym inżynierowie nie mogą być w wystarczającym stopniu paranoikami. Podobnie jak budowniczowie mostów chcą przekraczać coraz szersze rzeki i wąwozy, korporacje chcą rozszerzać swoje usługi w Internecie. Nakłada to ogromne ciśnienie na administratorów sieci. Proces ten będzie kontynuowany od miejsca gdzie system został zhackowany do miejsca w którym korporacje staną się bardziej konserwatywne. Jak wie każdy administrator firewalla, system jest pod ciągłym obstrzałem z Internetu. Hackerzy z całego świata stale polują na słabe punkty systemu. Co więcej, co kilka miesięcy pojawiają się nowe luki w bezpieczeństwie w popularnych produktach , w tym miejscu hackerzy po prostu skanują cały Internet szukając ludzi z takimi lukami, powodując tysiące włamań na strony.

6.3 Jeśli mam wykrywanie włamań czy potrzebuję firewalla?
Oczywiście. Każda korporacja potrzebuje dobrego zarządzania, pojedynczego punktu wejścia. Istnieje ogromna liczba "script-kiddies", którzy zawsze uruchamiają automatyczne programy (takie jak SATAN) przez Internet szukające dziur. Bez firewalla, programy te mogą wykryć i wykorzystać dziury dosłownie w oka mgnieniu. Również użytkownicy dial-up, którzy korzystają z Internetu tylko kilka godzin w tygodniu są skanowani na bieżąco; strony korporacyjne będą skanowane przez script-kiddies dużo częściej.

6.4 Skąd system wykrywania włamań pobiera informacje?Z firewalla?
Podczas gdy niektóre pliki dziennika programu do analizy logów firewalla są skanowane pod kątem włamań, większość systemów wykrywania włamań pobiera informcje gdzie indziej. Pamiętaj ,że firewalle są prostymi systemami zasad, które zezwalają / odrzucają ruch przez nie przechodzący. Nawet "kontola treści" firewalli nie jest w stanie jednoznacznie stwierdzić czy ruch stanowi atak; określa tylko czy odpowiada zasadzie czy nie. Na przykład firewall przed serwerem WWW może blokować cały ruch z wyjątkiem połączeń przez port 80. Jeśli chodzi o firewall, każy ruch na porcie 80 jest akceptowany. IDS , z drugiej strony ,bada ten sam ruch i szuka wzorcu ataku. IDS tak naprawdę nie obchodzi czy menadżer zezwolił na ruch na porcie 80 i odrzucanie reszty: jeśli chodzi o IDS cały ruch jest podejrzany. Oznacza to ,że IDS musi patrzyć na to samo źródło dancyh co firewall: mianowicie surowy ruch sieciowy na przewodzie. W powyższym przykładzie, firewall nigdy nie przepuści ruchu na porcie 80.



IDS #1

Kilka IDS'ów działa w ten sposób. Firewalle nie tworzą wystarczającej ilości informacji w celu skutecznego wykrywania włamań

IDS #2

To popularne umieszcznie IDS wykrywa ataki, które skutecznie przenikają przez zapory

IDS #3

To umieszczenie wykrywa ataki, które są próbą przeciwko firewallowi

IDS #4

Przez umieszczenie systemów wykrywania włamań w całej sieci firmowej, będą wykrywane ataki wewnętrzne.

VII. Przewodnik po implementacji

7.1 Jakie pytania powinenem zadać swojemu dostawcy IDS?

CSI (Coputer Security Institute) ma dobrą stronę w tym temacie, gdzie są stawiane pytania sprzedawcom IDS. Strona ta to http://www.gocsi.com/intrusion.htm

Niektóre pytania to:

Ile to kosztuje?

Oczywiście

Jakie są koszty aktualizacji sygnatur i utrzymania?

Wykrywanie włamań jest bardzo podobne do ochrony antywirusowej, system który nie był aktualizowany przez rok nie będzie odporny na nowe ataki.

Na jakim poziomie ruchu w świecie realnym produkt staje się ślepy, w pakietach / sekundę?

Po pierwsze jakie segmenty planujesz wprowadzić do IDS? Jeśli masz połączenie tylko 1.5 MB/s z Internetem, który chcesz monitorować, nie ma potrzeby szybszego systemu. Z drugiej strony, jeśli starasz się monitorowaćfarmy serwerów wswojej korporacji aby wykrywać ataki wewnętrzne, hacker może łatwo wykonać smurf aby oślepić czujnik. Najważniejsza metryka to pakiety/sekundę. Marketingowcy używają wielu słów aby mówić ,że ich produkt może nadążać przy pełnej 100 Mbps sieci, ale tylko w idealnych warunkach. Network Worls zrobił przegląd w sierpniu 1998 roku gdzie produkty nie nadążały przy 30% obciążeniu sieci (50 000 pakietów/sekundę) Podobnie Network Computing zrobił przegląd we wrześniu 1999 roku ruchu w świecie rzeczywistym, w którym kilka produktów twierdziło ,że może nadążyć przy 100 Mbps.

Jak jest skalowalny system IDS jako całość?

Ile czujników wspiera system? Jak duża może być baza danych? Jaki jest poziom ruchu w momencie przekazywania informacji do konsoli zarządzania?Co się dzieje gdy konsola zarządzania jest przeciążony? Są to trudne pytania

Ile będzie kosztowało uruchomienie i zarządzanie produktem?

Jak dobra jest architektura raportowania? Jak łatwo jest zarządzać fałszywymi alarmami? Jak długo trzeba czekać na śledzenie wpisów i określenia sytuacji? Ilu ludzi musi korzystać z tego produktu?

Poniższe pytania są często zadawane, ale jest mniejsze prawdopodobieństwo powstania znaczących odpowiedzi:

Ile podpisów wspiera system?

Niestety sprzedawcy zanacznie zawyżają swoje podpisy. Jest to gra w którą muszą grać wszyscy sprzedawcy,mimo, że jest to coraz mniej ważne

Jakie funkcje odpowiedzi posiada produkt?

Funkcja taka jak automatyczna rekonfiguracja firewalla brzmi naprawdę dobrze, ale w

prawdziwym życiu wdraża je kilku menadżerów bezpieczeństwa. Zmiana konfiguracji korporacyjnego firewalla jest bardzo niebezpieczna.

7.2 Jak utrzymywać na bieżąco system ?

Jeśli instalujesz system wykrywania włamań, będziesz widział włamania na bieżąco. W środowisku SOHO, będziesz prawdopodobnie otrzymasz skanowanie przez hackerów raz w tygodniu. Na dobrze znanych stronach WWW, hackerzy będą sondować twoją stronę pod kątem słabości wiele razy dziennie. W dużej, korporacyjnej sieci znajdziesz stale podejrzaną działalność prowadzoną przez wewnętrznych pracowników.. Pierwszym problemem przed jakim stają pracownicy jest surfowanie po stronach pornograficznych. Ciekawe jest ,że wiele konserwatywnych korporacji nie ogranicza bezwarunkowo takiego surfowania – bo często kierownictwo samo to robi. Inżynierowie niższego poziomu wykrywając taką działalność boją się podejmować ten temat. Kolejny problem jest taki ,że inżynierowie są problemem zasobów ludzkich (HR). Znajdziesz użytkowników robiących rzeczy , których nie powinni, więc sporo czasu spędzasz z pracownikami HR rozmawiając o sprawiających kłopoty pracownikach. Ostatni problem to co zrobić ze "script-kiddies" i hackerami badającymi systemu. Zazwyczaj połącz się z ISP e-mailem do ich skrzynki pocztowej "abuse@". Niektórzy ISP będą wdzięczni – ponieważ ich systemy zostały naruszone. Pamiętaj ,że to co wydaje się najbardziej rażącym hackowaniem może w rzeczywistości być niewinne.

7.3 Jak zatrzymać niewłaściwe surfowanie po Internecie?

Jednym z największych problemów dla firm są pracownicy sufrujący po "niewłaściwych" stronach internetowych. Do pewnego stopnia firmy obawiają się o pracowników marnujących czas w Internecie, obawiają się odpowiedzialności prawnej, np gdy pracownik surfuje po stronach pornograficznych, co może być odebrane jako molestowanie seksualne. Jednak firma nie chce być w sytuacji "Wielkiego Brata". Reguły skierowane przed niewłaściwym surfowaniem nieuchronnie prowadzą do szarej strefy (np Playboy.com niedawno miał artykuł na temat bezpieczeństwa komputerowego, na który mógł się natknąć pracownik poszukujący odpowiednich treści w sieci.). System wykrywania włamań, firewalle, serwery proxy i programy do sniffowania mogą być skonfigurowane do logowania całego ruchu przeglądania stron, do dzienników pliku. Większość firm już ma takie dzienniki, ale mało kto używa tych informacji. Technicy sieciowi nie chcą brać na siebie roli HR i organów ścigania . Jednym z eleganckich rozwiązań jest delegowanie takich informacji do wewnętrznej publicznej strony. To może jakoś wpłynąć na niewłaściwe surfowanie.

7.4 Jak zbudować własny IDS (pisanie kodu)?

Proste systemy wykrywania włamań są łatwe do zbudowania.Wystarczy pobrać źródła sygnału (pliki rejestrowe, ruch w sieci) i przekazać je przez dopasowanie wzorca (regexp). Wraz z nimi, te same dane poprzez analizę statystyczną, taką jak SETI@Home, wysyłamy zakłócenia radiowe przez analizę Fouriera szukając powtarzających się wzorców. Na przykład omawialiśmy wcześniej system "network grep", który przekazywał ruch sieciowy poprzez system dopasowania wzorców. Taki system może być zbudowany o pewną wiedzę o języku C i systemu UNIX. Omawialiśmy również system oparty o PEARL, który analizował pliki rejestrowe z firewalla.

7.5 Jaka jest zgodność z prawem NIDS (ponieważ jest formą podsłuchu)?

Różne kraje mają różne prawa, ale jest ogólnie prawne monitorowanie WŁASNEGO ruchu przeciw włamanią/ Jednym z problemów jest to ,żę ludzie wiedzą o uruchomionym NIDS w sieci korporacyjnej a administratorzy sieci monitoruję przeglądanie Internetu przez pracowników. Ponieważ wysposażenie sieciowe i stacje robocze użytkowników należą do firmy, prawnym precedensem jest to ,że używanie wyposażenia firmowego oznacza zgodnę na monitoring. Jednak zaleca się aby firmy wyraźnie muszą zaznaczać ,że działalność w sieci będzie monitorowana. Aby unikną kłopotliwych sytuacji.

7.6 Jak zapisywać pliki rejestracyjne w sposób zabezpieczony przed manipulacją?
Pierwszą rzeczą jaką robi hacker jest usuwanie / zmienianie plików logowania w celu ukryciaa dowodów na włamanie. W związklu z tym zalecane jest posiadanie systemu "jednokrotnego zapisu", gdzie dane są zapisywane ale nie można ich zmienić. Dyski WORM (Write-Once-Read-Many) były w przeszłości wykorzystywane w ten sposób,ale były za drogie. Prawdopodobnie nie mają sterowników do twojego systemu a i oprogramowanie prawdopodbnie jest z nimi niekompatybilne w inny sposób. Jednym z problemów jest to że każdy system jest zbiorem entropii. Może być bezpieczny dzisiaj, ale nie jest powiedziane ,że na tym się skończy. Na przykład, jedna technika logowania może wykorzystywać syslog gdzie odbiorca nie ma stosu TCP/IP ale używa tcpdump do zapisywania surowych pakietów do pliku (prawdopodobnie narzędzie będzie uruchamiane później do rekonstrukcji pozycji syslog. Z punktu widzenia entropii, nie ma gwarancji ,że stos TCP/IP nie będzie instalowany podczas aktualizacji, lub kiedy nowa osoba dołącza do zespołu, lub gdy komputery są przemieszane. Aby zwalczać takie entropie, model systemu używa podejścia "snipped-wire". W tym modelu instalowana jest dodatkowa karta Ethernetu w komputerze który generuje dane, a odbierzesz cięcie przewodu. Jeśli później wydarzy się wypadek tak ,że jest połączony dodatkowy adapter do niezabiezpieczonej sieci, wtedy wystąpi kilka problemów. W taki sam sposób, system odbioru powinien mieć tylko pojedynczą kartę Ethernetową, a jej przewody transmisyjne powinny być ucięte. Najlepiej byłoby aby również wyłączyć stos TCP/IP a zamiast tego wymusić dane poprzez narzędzia do sniffowania pakietu. Normalny TCP/IP nie działa w tym scenriuszu. Będziesz potrzebował ustalonej drogi i tablic ARP na komputerze generującym aby wymusić ruch jednikierunkowy. Podobnie będziesz musiał użyć specjalnego narzędzia na komputerze odbiorczym aby analizować pakiety przychodzące z powrotem do użytecznych danych 'syslog; i SNMP Traps są najczęściej używanymi środkami transportu w tej sytuacji. Są one łatwe do wygenerowania na maszynach wychodzących, ponieważ są wbudowane w większość systemów. Ponieważ odpowiedz nie są generowane tak czy tak,nie zakłoca to normalnego przepływu aplikacji. Podobnie ,są łatwe do analizy z powrotem do wiadomości SNMP lub plików syslog w miejscu docelowy, lub przynajmniej łatwo jest wzmocniż stos TCP/IP dla odbierania tylko tych portów. W każdym razie TFTP lub NTF mogą być skonfigurowane do transportu plików do stosu TCP/IP po drugiej stronie. Problemem , któy z tym idzie w parze jest zarządzanie danymi. Nie można połączyć repozytorium danych z siecią, więc wszystko potrzebne do tworzenia kopii zapasowej musi być zainstalowane na samym systemie.

VIII. Jakie są ograniczenia NIDS

Systemy wykrywania włamań sieciowych są wiarygodne na tyle, że należy je traktować jedynie jako układy pomocnicze przeznaczone do tworzenia kopii zapasowych podstawowych systemów bezpieczeństwa. Podstawowe systemy takie jak firewalle, szyfrowanie i uwierzytelnianie są solidne. Błędy lub błędna konfiguracja często prowadzą do problemów w tych systemach, ale podstawowe pojęcia są dokładnie "dające się udowodnić". Podstawowe pojęcia poza NIDS są absolutnie prawdziwe. Systemy wykrywania włamań cierpią z podowu dwóch problemów przy czym normalny ruch powoduje wiele fałszywych alarmów i ostrożni hackerzy mogą unikać lub wyłączać system wykrywania włamań. Rzeczywiściw, istnieje wiele dowodów, które pokazują jak systemy wykrywania włamań mogą być niedokładne. Nie znaczy to ,że systemy wykrywania włamań są nieważne. Hacking jest tak wszechobecny w dzisiejszej Sieci ,że ludzie są regularnie zdumienie,gdy po raz pierwszy instalują takie systemy (wewnątrz i na zewnątrz firewalla) Dobry system wykrywania włamań mogą dramtycznie poprawić bepieczeństwo strony. Trzeba po prostu zapamiętać ,że systemy wykrywania włamań są kopią zapasową.

8.1 Sieci komutowane (nieodłączne ograniczenia)
Sieci komutowane (takie jak 100 Mb/s i komutowany Gihgabit Ethernet) stawia dramtyczne problemy z systemami wykrywania włamań sieciowych. Nie jest łatwo umieścić "wtyczkę" czujnika aby zobaczyć cały ruch.

Osadzony IDS wewnątrz przełącznika
Niektórzy producenci (Cisco, ODS) osadzają wykrywanie włamań bezpośrednio w przełącznikami. O ile wiem, jednak, te systemy IDS nie mają szerokiego zakresu wykrywnia tak jak tradycyjne NIDS.

Monitorowanie portu
Wiele przełączników ma "port monitora" dla podłączania analizatorów sieci. NIDS moze być łatwo dodany również do tego portu. Oczywistym probleme jest to ,że port działa ze znacznie mniejszą prędkością niż przełącznik na płycie tylnej, więc NIDS nie będzie mógł zobaczyć całego ruchu na mocno obciążonym przełączniku. Ponadto, takie porty są często używane przez sniffery dla celów zarządzania siecią, i często muszą być przełączane sporadycznie.

Dotknięcie kabla
Monitor może być podłączony bezpośrednio do kabla aby aby monitorować ruch. Mogą to być kable między przełącznikami lub kablami od przełącznika do hosta. Można zastosować różne techniki:

rozgałęźnik inline
Zawory inline są urządzeniami, które są wstawione bezpośrednio do strumienia komunikacyjnego i robią jej kopię. Typowym przykładem będzie Shomiti Century Tap, który podłącza się do 100 Mbps linii full duplex, i pozwala na komputer wypsoażony w 2 karty do odczytu obu kanałów.

rozgałęźnik wampir
Dawniej, rozgałęźniki wampiry były podstawą grubego kabla koncetrycznego Ethernetu i były preferowanym sposobem łączenia węzłów końcowych sieci.

rozgałęźniki indukcyjne
Większość rozgałęźników może być wykryta przez wyposażenie TDR (Time Domain Reflectometr). Rozgałęźniki indukcyjne robią zmiany na kablu aw dowolny sposób, ale zamiast miejsca na zewnątrz i monitorowania zakłoceń elektromagnetycznych emitowanych przez przewody. Używane tylko przez szpiegów.

Problem z podsłuchem kabla zwłaszcza między przełącznikami, jest to ,że generują dużą ilość ruchu. Większość NIDS nie mogą obsługiwać bardzo dużego obciążenia przed pójściem w "ciemno".

Czujniki oparte na hoście
Z koncepcyjnego punktu widzenia, jedynym sposobem na pokonanie ograniczeń sieci komutowanych jest dystrybucja wykrywania włamań opartych o host. Kilka takich agentów, jak BlackICE i CyberCop Monitor, zawierają komponenty sieciowe, które monitorują tylko ruch na hoście. Inne robią tradycyjne pliki rejestracyjne i analizę audytu

8.2 Ograniczenia zasobów
Systemy wykrywania włamań sieciowych usadowione są w scentrolizowanym miejscu w sieci. Muszą być w stanie utrzymać się z analizy, i przechowywania informacji generowanych przez potencjalne tysiące komputerów. Musi emulować połącznie wszystkich komputerów wysyłających ruch przez segment. Oczywiście, nie może zrobić tego w pełni, i musi iśc na skróty.

8.2.1 Ładowanie ruchu sieciowego

Obecne NIDS mają problemy z nadążaniem za w pełni zaladowanymi segmentami. Średnia strona internetowa ma 180 bajtowy rozmiar ramki, co przekłada się na 50 000 pakietów na

sekundę przy 100 Mbps Ethernecie. Większość IDS nie może nadążyć z tą prędkością. Większość klientów ma jednak mniej niż tyle. Przy zakupie IDS ,zapytaj sprzedawcę ile pakietów na sekundę może obsłużyć. Wielu dostawców próbuje powiedzieć ile bitów na sekundę ale na pakiet jest rzeczywistą wydajnością "wąskiego gardła". Praktycznie wszyscy producenci mogą obsługiwać 100Mb ruch przy użyciu 1500 bajtowych pakietów, kilka jest w stanie obsłużyć 100Mbps ruch przy 60 bajtowych pakietach

8.2.2 Połączenia TCP

IDS musi zarządzać stanem połączenia dla dużej liczby połączeń TCP. Wymaga to rozszerzonej ilości pamięci. Problem ten nasila się przez techniki oszustw, co często wymaga aby IDS zarządzał informacją o połączeniu nawet po zamknięciu połączenia klient / serwer. Przy zakupie IDS, spytaj sprzedawcę ile równoczesnych połączeń TCP może obsłużyć.

8.2.3 Inne informacje o stanie

TCP jest najprostszym przykładem informacji o stanie, które muszą być przechowywane przez IDS w pamięci, ale inne przykłady to fragmenty IP, informacje skanowania TCP i tablice ARP

8.2.4 Stan długotrwały

Klasycznym problemem jest "wolne skanowanie", gdzie atakujący skanuje system bardzo powoli. IDS nie jest w stanie przechowywać informacji przez dłuższy czas, więc nie może dopasować danych razem

8.3 Ataki przeciwko NIDS

Systemy wykrywania włamań same mogą być atakowane w następujące sposoby

8.3.1 Zamaskowanie czujnika

Systemy wykrywania włamań sieciowych są generalnie budowane jako "pasywne monitory" z komputerów COTS (commercial-off-the-shelf (prosto z półki)). Monitory są umieszczane obok strumienia sieciowego, nie w środku. Oznacza to ,że jeśli nie mogą nadążyć za wysokim poziomem ruchu, nie mają sposobu aby puścić go ponownie. Muszą zacząć zmniejszać pakiety. Jest to znane jako picie z wężą strażackiego. Niewiele NIDS dzisiaj może nadążyć za wpełni nasyconym łączem 100 Mbps (gdzie "nasycony"oznacza średniej wielkości paczki 180 bajtów, czyli około 50 000 pakietów/sekundę). Nie tylko czujniki zaczynające zmniejszać pakiety nie przetwarzają, wysoki ruch może całkowicie wyłączyć czujnik. Na przykład rozważmy czujnik, który może przetwarzać maksymalnie 20000 ramek na sekundę. Kiedy ładowanych jest 40 000 ramek/sekundę, zazwyczaj zmniejszasie aktualne przetwarzanie do 10000 ramek na sekundę lub 5000 ramek na sekundę lub nawet do zera. Jest tak ponieważ ramka odbioru i ramkla analizysą dwiema różnymi działaniami. Większość architektur wymaga aby system do przechwytywania pakietów, nawet gdy jest zbyt zajęty aby je analizować. Dlatego intruz może zaatakować czujnik przez nasycenie łącza. Jeśli intruz jest lokalny, on/ona może po prostu z transmisji programu. 400 Mhz pole może w pełni nasycić łącze z pakietami 60 bajtowymi, łamiąc większość systemów IDS, które mogą być podłączone do systemu. Zdalny atakujący może wykonać atak smurf lub fraggle, podobnie nasycając łącze.. Jest mało prawdopodobne ,że atakujący będzie miał dość szybkie łącze (100 Mbps zdarza się rzadko) aby być w stanie zaatakować w ten sposób.

8.3.2 Zamaskowanie przechowywania zdarzeń (ślepy śnieg)

Narzędzie do skanowania portów 'nmap' zawiera funkcję zwaną jako skanowanie "decoy". Skanowanie używające setek sfałszowanych adresów źródłowych jak również realnych adresów IP atakującego. Staje się zatem nieprawdopodobnym zadaniem dla administratora

znalezienie które adresy IP są przwdziwe, a które są adresami na wabia. Każdy atak może być zbudowany z tych samych komponentów. Masowy atak sfałszowanymi atakami może zawsze ukryć prawdziwy atak dodanego gdzieś w środku. Administratorom będzie ciężko odkryć prawdziwy atak wewnątrz tego całego szumu. Te dwa scenariusz zachowują jeszcze dane sądowe. Jeśli atakujący jest podejrzany, daną jeszcze tam można znaleźć. Inny atak to wypełnienie pamięci zdarzeń. Gdy baza danych jest wypełniona,żaden atak nie będzie wykryty, lub wykrywane będą usuwane. Tak czy inaczej nie istnieją żądne dowody na to ,że wszędzie można będzie wskazać intruza.

8.3.3 Denial of Service (DoS)

NIDS jest niezwykle złożonym systemem o równoważnej złożoności całego stosu TCP/IP z działajacymi wieloma usługami. Oznacza to ,że NIDS jest podatny na takie taki jak SYN flood czu smurf. Ponadto liczne protokoły anaizy NIDS pozostawiają go otwartym na zawieszenie się podczas niespodziewanego ruchu online. Napstnik może często kupić taki sam system wykrywania włamań używany przez jego ofiary, potem eksperymentować na wiele sposobów aby znaleźć pakiety które zabiją IDS. Podczas takiego ataku intruz zbija IDS, i dalej pozostaje niezauważonym.

8.4 Proste uniki

Tu opiszę proste taktyki unikania, które oszukają podstawowe systemy wykrywania włamań.

8.4.1 Fragmentacja

Fragmentacja jest to możliwość podział pojedynczego pakietu IP na wiele mniejszych pakietów.. Stos odbioru TCP/IP składa je potem z powrotem przed przekazaniem danych z powrotem do aplikacji. Większość systemów wykrywania włamań nie ma możliwości ponownego składania pakietów IP. Dlatego istnieją proste narzędzia (jak gragroute), które mogą automatycznie fragmentowaćatak w celu oszukania IDS. Zauważ ,że framgmentacja pakietów IP w środku nagłówka TCP od dawna jest używane aby uniknąć filtrowania przez port firewalla. Niektóre przemysłowe klasy NIDS mogą składać ponownie ruch. Również niektóre firewalle mogą "normalizować" ruch przez wymuszanie ponownego składania przed przekazaniem ruchu do drugiego końca.

8.4.2 Domyślne unikanie

Ludzie często używają firewalli jako łatwego NIDS, gdzie czynią założenia ,że port przeznaczenia jednoznacznie identyfikuje ten protokół Hacker który skutecznie zainstaluje tylne drzwi może uruchamiać standardowe protokołu na portach niestandardowych. Na przykład, hacker może wysłać użytkownikowi zainfekowany program Back Orifice, ale zmienia port z domyślnego 31337. Sporo systemów wykrywania włamań nie będzie już prawidłowo identyfikować ruchu (choć nieliczne).

8.4.3 Wolne skanowanie

Ze względu na natężenie ruchu, NIDS mają trudności z utrzymaniem długoterminowych dzienników ruchu. Dlatego też trudno wykryć "wolne skanowanie" (wymiatanie ping czy skanowanie portów) gdzie intruz skanuje jeden port / adres co godzinę.

8.4.4 Skoordynowany atak niskiej przepustowości

Czasami hackerzy zbierają się razem i uruchamiają wolne skanowanie z wielu adresów IP. Utrudnia to systemowi wykrywania włamań do powiązania tych informacji.

8.4.5 Adres spoofing / proxying

Jednym z celów wykrywania włamań jest wskazanie palcem, kto cię atakuje. Może to być trudne z wielu powodów. W ataku "Smurf", na przykład, pojawia się tysiące odpowiedzi z

pakietu, który nigdy nie został wysłany. NIDS wykrywa te odpowiedzi ale nie może odkryć kto wysłał sfałszowany pakiet. W TCP Sequence Number Prediction sfałszowane adresy IP są używane tak ,że NIDS nie zna dokładnie, skąd intruz nadejdzie. W końcu, większość intruzów odbija swoje ataki za pomocą protokołu FTP lub sieciowych serwerów proxy, lub z innych stron, na które się już włamali. Zatem bardzo trudno powiedzieć kto atakuję twoją stronę a konfiguracja filtra adresów IP w firewallu nie pomoże.

8.4.6 Uchylanie się za pomoca zmiany wzorca

Wiele prostych systemów wykrywania włamań sieciowych powołuje się na "dopasowanie do wzorca" Skrypty ataków mają dobrze znane wzorce, więc prosta kompilacja danych wyjściowych bazy danych dobrze znanych ataków skryptowych zapewoa bardzo dobre wykrywanie, ale może być łatwo ominięte przez prostą zmianę skryptu. Na przykład niektóre serwery POP3 są narażone na przepełnienie bufora kiedy wpisywane jest długie hasło. Istnieje kilka popularnych ataków skryptowych dla tej luki. Jeden system wykrywania włamań może zawierać 10 dopasowanych wzorców, wzorce do 10 najpopularniejszych skryptów, podczas gdy inne przyglądają się polu wpisywania hasła i alarmują kiedy zostało wprowadzonych więcej niż 100 bajtów. Pierwszy system jest łatwy do oszukania po prostu przez zmianę skryptu ataków, podczas gdy drugi system przechwytuje dowolny atak w tym miejscu. Typowym przykładem jest prosta zmiana adresu URL. Chociaż dokładny wzorzec zostanie zmieniony, znaczenie nie zostało zmodyfikowane .

8.5 Unikanie złożone

Utalentowani hackerzy mogą kierować swoje ataki na swoje ofiary w taki sposób ,żeby ominąć system wykrywania włamań. Na przykład, intruz może wysłać pakiet TCP FYN, które widzi NIDS, ale którego nie widzi host ofiary. Powoduje to ,żę NIDS sądzi ,że połączenie jest zamknięte, ale w reczywistości tak nie jest. Ponieważ połączenie TCP nie wysyła "podtrzymania", intruz może czekać godziny lub dni po tym "zamknięciu" przed kontynuacją ataku.W praktyce, większość ciekawych usług zabije połączenie po upływie pewnego czasu bez aktywności ale intruz jeszcze może poczekać kilka minut przed kontynuacją . Pierwszym takim atakiem jest znalezie sposobu przekazania pakietów do NIDS, ale powoduje to w przyszłości router odrzuca pakiety. To zależy od konfiguracji routea, ale typowy przykład zawiera niskie pola TTL, fragmentację, źródło routingu i inne opcje IP. Jeśli jest wolne łącze przez NIDS, wtedy hacker może floodować to łącze z wysokim priorytetem pakietów IP i przesyła TCP FIN jako pakiet o niskim priorytecie – mechanizm kolejkowania routera prawdopdobnie zrzuci pakiet. Innym podejściem jest rozważenie, jaki host będzie lub nie akceptowany. Na przykład, różne stosy TCP zachowują się odmiennie dla lekkio niepoprawnych danych(których to programy takie jak 'nmap' i 'queso' używają jako odciski palców w systemie operacyjnym). Typowym sposobem wykorzystania różnego ruchu jest przyjęcie / odrzucenie opcji TCP, spowodowanie wystąpienia limitu czasowego dla framgentów IP lub segmentów TCP, pokrycie fragmentó / segmentów, wysłani niewielkiej błędnej wartości flag TCP lub sekwencji liczb. Zauważ na przykład, że jeżeli pokrywające się fragmenty są wysyłane z różnych danych, niektóre systemy wolą dane z pierwszego fragmentu (WinNT, Solaris), podczas gdy inne przechowują dane z ostatniego fragmentu (Linux, BSD). NIDS nie ma sposobu dowiedzenia się który węzeł końcowy będzie zaakceptowany i może odgadnąć źle. Analiza połączenia TCP była głębsza, przy omawianiu "desynchronizacji" połączenia TCP, co jest bardziej wrażliwe niż mogłoby się wydawać, Ponownie IDS nie może porawnie modelować wszystkich możliwych zachowań stosu TCP/IP i dowiedzieć się jaki węzeł końcowy będzie akceptował dane. TCP ma również problemy pokrywania, które ma frmagmentacj IP. Na przykład system wykrywania włamań moze akceptować pierwszy segemnt i ignorować dalsze segmenty ale większość hostów akceptuje późniejsze segmenty. Wyniki testów systemów wyrywania włamań okazały się porażające. Jeden główny system wykrywania włamań może być całkowicie ominięty przez pofragmentowane pakiety, inne przez "desynchronizację" danych z akceptowanego węzła końcowego.

8.6 Narzędzia

Poniższe narzędzia mogą być pomocne w ocenie systemów IDS pod kątem tych problemów.

Anzen NIDSbench

Zawiera "fragrouter" , któy zmusza do fragmentacji całego ruchu, i któy pokazuje jak łatwo hacker / cracker zrobi to samo aby ominąć wykrywanie włamań. Akceptuje ruch przychodzący potem fragmentuje goi według różnych zasad(fragmentacja IP z różnymi rozmiarami i nakładaniem, ponowna segmentacja TCP z różnymi rozmiarami i nakładkami,wkładka TCP aby desynchronizować połączenia itp). Zawiera również program "tcpreplay", któy zrzuca duże obciążenie na segment Ethernet aby zweryfikować możliwości nadążania NIDS.

CASL

NAI CyberCop Scanner jest wyposażony we wbudowany CASL. Umożliwia on obsługę skryptowania na niskim poziomie pakietów TCP/IP

IX.System pułapek i podstępów

Chociaż nie jest to ściśle mówiąc system wykrywania włamań oparty o sniffer, pułapki przetwarzają jeszcze protokoły sieciowe w podobny sposób

9.1 Co to jet pułapka?

Pułapka jest to system zaprojektowany z myślą o tym ,ze intruz może go zhackować. Przykładami mogą być:

- Instalacja komputera w sieci bez określonego celu innego niż logowanie wszystkich prób dostępu
- Instalacja starszego ,niepoprawionego, systemu operacyjnego na komputerze. Na przykład domyślna instalacja WinNT 4 z IIS4 może być zhackowana przy użyciu kilku różnych technik. Standardowy system wykrywania włamań może być potem uzyty do logowania hacków skierowanych przeciwko komputerowi, a później śledzenie co intruz próbuje zrobić w systemie , który jest już zarażony
- Instalacja specjalnego oprogramowania stworzonego do tego celu. Ma to tę zaletę, że wygląda ,że intruz zakończył włamanie z powodzeniem bez rzeczywistej zgody na dostęp.
- Każdy istniejący system może być "upułapkowany". Na przykład, na WinNT możliwa jest zmiana nazwy domyślnego konta "administrator", potem stworzenie dowolnego konta nazwanego "administrator" bez hasła. WinNT umożliwa szerokei rejestrowanie działalności osób, więc pułapka będzie śledzić użytkowników próbujących uzyskać uprawnienia administratora i wykorzystać ten dostęp.

9.2 Jakie są zalety pułapki?

Wczesne ostrzeganie o wrogiej działalności. Systemy wykrywania włama sieciowych mają problem z odróżnieniem wrogiego ruchu od ruchu właściwego. Wyizolowane pułapki mają dużo łatwiej ponieważ są systemami, które normalnie nie są dostępne. Oznacza to ,że cały ruch do systemu pułapki jest już podejrzany. Narzędzi do zarządzania i oceny sieciowych zagrożeń są w dalszym ciągu przyczyną fałszywych alarmów, ale dają inny lepszy wskaźnik wykrywalności.

System oceny wrogich intencji. Pułapki często przedstawiają się jako łatwe do zhackowania systemy. Jedną z najczęstszych rzeczy jakie robi hacker to skanownie Internetu robiąc "banner cheks" .Pułapka może być ustawiona tak aby dostarczyc banner tak, aby wyglądał jak system który może być łatwo zhackowany. Na przykład usługa POP3 raportuje werdję oprogramowania. Niektóre wersje dobrze znanych pakietów mają dziury przepełenienia bufora. Hacker łączy się do portu 110, przechwytuje informację o wersji z bannerem, potem sprawdza wersję w tabeli, która wskazuje jaki skrypt można wykorzystać do włamania do systemu.

9.3 Jakie są wady pułapek?

- Jeśli system rzeczywiście został shackowany, może być używany jak odskocznia do dalszych włamań sieciowych
- Niektórzy ludzie wierzą ,że ponieważ pułapki przyciągają hackerów, prawa do ścigania hackerów są zredukowane. To nieporozumienie, ponieważ pułapki nie są aktywnymi przynętami – nie rekalmują się Hacker może tylki znaleźć pułapkę uruchamiając programy do wyszukiwania w sieci
- Pułapki dodają złożoności. W bezpieczeństwie, złożoność jest zła: prowadzi do zwiększonego narażenia się na ataki
- Pułapki muszą być zarządzane podobnie jak inne sieciowe urządzenia / usługi. Prowadzi to wielu ludzi do ich wyłączenia po pewnym czasie. Myślisz ,że 486 z systemem RedHat Linux 4.2, który 2 lata temu był konfigurowany nie wymaga konserwacji? Skąd wiesz ,że rejestrowanie jest działaniem prawnym? Co zorbić kiedy nowa platforma zarządzania siecią i system oceny przydatności zaczynają być używane i uruchamiają alarmy? Co zrobić kiedy alarmy zaczynają przychodzić ponieważ hacker złamał ten system i używa go do uruchamiania ataków przeciwko tobie (lub co gorsza, z powrotem w Internecie)?

9.4 Jak mogę skonfigurować swoją własną pułapkę?

Należy pamiętać ,że ustawienie pułapki jest naprawdę proste. Podczas gdyu prodykty pułapek są naprawdę fajne, praktycznie każde istniejące urządzenie / oprogramowanie może być ustawione jako twoja pułapka. Twój plan powinien się składać z następujących kroków:

dokumentacj, dokumentacja, dokumentacja

Pierwszym krokiem w we wszelkich staraniach zarządzania siecią (faktycznie, w ostatnim etapie ludzie odkrywają swój ból, że nie zrobili tego pierwszego kroku)

plan konserwacji

Jak planujesz go utrzymywać?

raportowanie alarmów

Jak cchesz otrzymywać alarmy z systemu?

plan reakcji

Co masz zmaiar zrobić po nadejściu alarmu?

9.5 Jakie są typy pułapek?

Monitory portów

Najprostszą pułapką jest po prostu program oparty o gniazda, który otwiera się na nasłuchiwanie na portach. Typowym przykładem tego jest NukeNabber (dla Windows) , któy nasłuchuje na portach zazwyczaj skanowanych przez hackerów. Alarmuje on użytkownika które z nich są skanowane. Wadą tego programu są;

- W większości przypadków są one używane, to rzeczywiście lepiej skonfigurować firewall aby zablokować napastnikowi dostęp. Monitorowanie portów nie rejestruje lepiej niż firewall
- Alarmuje hackera ,że taki system jest uruchomiony ponieważ najpierw akceptują a potem odtrzucają połączenie

Oszukańczy system

Kolejnym logicznym krokiem za monitorowaniem portów jest system który rzeczywiście współdziała z hackerem. Na przykład, zamiast po prostu zaakceptować port 110 dla POP3, następnie go opuszcza, oszukańczy system rzeczywiście reagowałby tak jeśli byłby serwerem POP3. Ponieważ 99% ataków przeciwko POP3 to bufferoverruns w nazwie użytkownika lub haseł, większość oszukańczych systemów tylko implementuje tą część protokołu. Podobnie, większość oszukańczych systemów implementuje tylko tyle protokołu komputera niezbędnych do pułapek w 90% ataków przeciwko protokołowi

Wieloprotokołowe systemy oszukańcze

Pakiety takie jak Specter lub Fred Cohen's Decetpion Toolkit oferują większosć popularnych protkołów hackerskich w pojedynczym zestawie narzędziowym. Podobnie, systemy te przychodzą z wieloma bannerami aby emulować pakiety dla różnych systemów operacyjnych

Pełne systemy

Oprócz systemów przeznaczonych bezpośrednio do oszustw, można również zaimplementować pełne systemy. Większość systemów posiada zdolność do alarmowania o warunkowych wyjątkach. Korzystają z wbudowanego natywnego logowania / audytowania

Pełny system plus NIDS

Pełny system, o jakim wspomniałem powyżej może zawierać również pełny system wykrywania włamań sieciowych uzupełniający wewnętrzny dziennik rejestrowania.

9.6 Jakie są plusy i minusy stworzenia systemyu, który może zostać shackowany?

Trzy najczęściej hackowane systemy w sieci są to niepoprawione systemy urucomione ze starszym Linuksem(jak redHat 5.0), Solaris 2.6 i Microsoft IIS 4.0. Dlatego jako część swojego planowania pułapki możesz skonfigurować jeden lub wszystkie z tych trzech systemów.

Pamiętaj: Jeśli umieścisz jeden z tych systemów w Internecie, w ciągu miesiąca zostanie odkryty i zhackowany

Plusy:

Więcej informacji na temat częstości występowania reakcji

Większośćludzi wierzy, że "im się nic nie stanie" i są nieprzygotowani keidy się to wydarzy. Skonfigurowanie systemów na które włamią się hackerzy nauczy cię jak wykrywać włamania i jak po nich posprzątać.

Więcej informacji o technikach hackerskich

Podglądanie włamań hackerów do systemu uczy wiele o hackingu. Jeśli potrzebujesz bezpiecznego systemu wewnątrz firmy (na przykład takiego, który posiada informacje finansowe) ustaw podobny system na zewnątrz firmy z fikcyjnymi danymi. Jeśli hacker złamie ten system, dowiesz się jak chronić wnętrze firmy przed podobnymi atakami.

System wczesnego ostrzegania

Konfiguracja serwerów wewnątrz firmy, które można łatwo zhackować będzie cię alarmowała o wrogiej działalności na długo przed rzeczywistym zagrożeniem systemu. Hackerzy próbują najpierw prostszych technik zanim przejdą do trudniejszych sposobów włamania do systemu. Dlatego stworzenie łatwo hackowalnego systemu będzie wskazywało wyraźnie na czyjeś złe zamiary.

Minusy:

Punkt uruchomienia

Największym niebezpieczeństwem jest to ,że ktoś może używać tego systemu do uruchamiania dalszych ataków na ciebie lub innych ludzi. W szczególności mogą być uwarunkowania prawne kiedy system atakuje trzecią stronę.

9.7 Jakie są środki zaradcze przeciwko oszustwom?

Poza pułapkami, możesz ustawić "środki zaradcze przeciwko oszustwom". Z twojej sieci "wycieka" wiele informacjio tobie, których hacker użyje we włamaniu do twojej sieci. Dlatego, jeśli przecieki są nieprawdziwe o sieci, wtedy udzielanie fałszywych informacji napastnikom. Można to zrobić w następujące sposoby:

Nagłówki e-mail

Klasycznym problemem w sieci, jest to ,że wiadomość e-mail wstawia adres IP systemu wysyłającego wiadomość do niej. Jeśli jesteś wewnątrz korporacji i wysyłasz e-mail, ujawniasz wewnętrzne serwery e-mail. Jeślu używasz jakiegos darowego systemu, adres IP komputera użytego do wysyłania wiadomości znajduje się w nagłówku. Proces ten trwa głębiej ponieważ e-mail wewnątrz firmy często podróżuje przez bramy, firewalle i skanery antywirusowe treści. Jest to trudne, ale może przeprogramować to aby wstawiać fałszywe adresy IP do nagłówka

Informacja DNS

Jedną z pierwszych rzeczy jaką robi hacker jest DNS Zone Transfer. Wielu administratorów blokuje dostęp do portu 53 TCP aby to zatrzymać (chociaż zatrzyma to również inne usługi DNS) Przez dodanie fałszywych komputerów lub nawet całych fałszywych subdomen można podać fałszywe dane hackerom. Na przykład mogę skonfigurować komputer z adresem IP 192.0.2.132, co powie mojemy IDS'woi ,żebyu się uaktywniał kiedy zobaczy ruch do tego adresu. Ponieważ mój IDS wyzwala się w Zone Transfer, złapie każdego kto poważnie próbuje zakłócić zakres mojej sieci.

anty-sniffer

Czy jesteś pewny ,że twój ISP cię nie sniffuje? Cóż, aby to sprawdzić , skonfiguruj komputer gdzieś w Internecie aby połączyć kilka twoich pól używając haseł jawnych. Potem ustaw swój IDS aby uaktywniał się gdy ktoś jeszcze używa tego hasła. Najlepiej zastosować pułapkę, która nie ma prawdziwych usług. Na przykład, skonfigurowałem wirtualnego demoan Telnet tak ,że inne komputery logują się do niego. Skonfigurowałe IDS aby uaktywniał się jeśli ktoś loguje się używając tego konta. Po zalogowaniu szybko się dowie ,że nie jest to prawdziwe konto.

anty sniffer , część druga

Podobnie jak powyżej, możesz przesłać plik z hasłami przez sieć, które zawierają łatwo łamliwe hasła, potem aktywuj IDS kiedy ktoś próbuje się zalogować. Na przykład, skonfiguruj plik wsadowy, który regularnie przesyła pliki przez FTP, z których jedne jest plikiem /etc/passwd. Dzięki temu dowiesz się czy ktoś nie sniffował tego pliku.