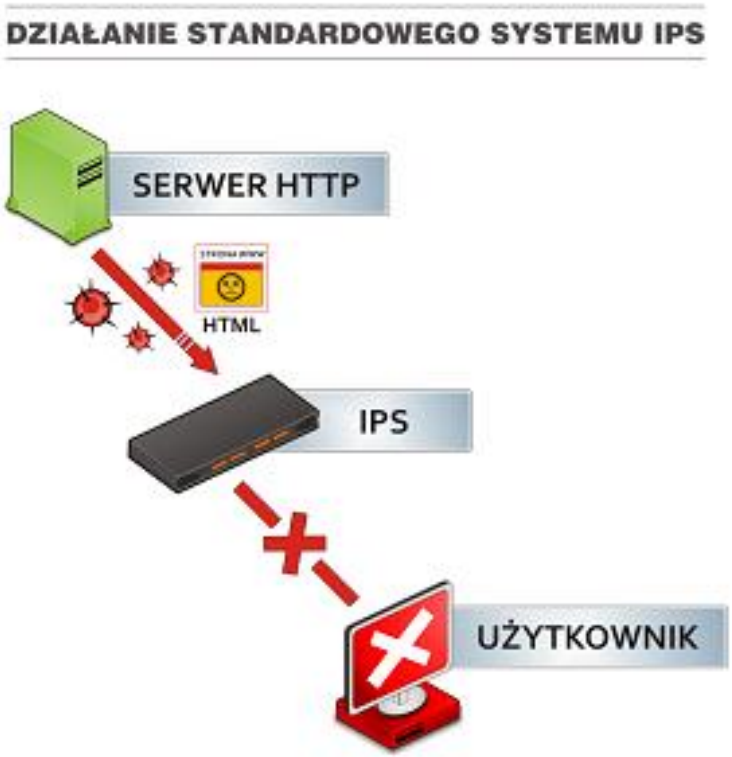
Eksploatacja i bezpieczeństwo systemów

dr inż. Mirosław Mazurek

Zakład Systemów Złożonych
Bud. F, pok. 305, tel. 17 865 11 04

Wykrywanie intruzów

IDS, IPS (ang. Intrusion Detection System, Intrusion Prevention System – systemy wykrywania i zapobiegania włamaniom) – urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym.



Zbieranie informacji

Celem tego typu testów jest empiryczne określenie odporności systemu na ataki. Testy penetracyjne mogą być prowadzone z wnętrza badanej sieci oraz z zewnątrz. Testy zewnętrzne są zwykle realizowane przez ludzi, którzy nie znają penetrowanego systemu. Nie znają szczegółów jego topologii konfiguracji i zabezpieczeń. W przypadku realizacji testów należy liczyć się z możliwością załamania systemu. Nie może to być jednak czynnik ograniczający zakres badań i powodujący realizację zbyt ostrożnych testów. Przez takimi badaniami należy przede wszystkim utworzyć nowe, pełne kopie zapasowe.

Test penetracyjny rozpoczyna się zwykle od zebrania informacji o systemie poza nim samym. Może obejmować analizowanie pakietów rozgłoszeniowych, badanie DNS, uzyskiwanie danych u dostawcy usług internetowych przeszukiwanie publicznych zbiorów informacji jak WWW czy LDAP.

Wykrywanie intruzów

Jest to proces przebiegający w czasie. Obejmuje technologię, ludzi i narzędzia.

Identyfikację intruza można przeprowadzić przed, podczas lub po wystąpieniu działalności szkodliwej.

Działalność zapobiegawcza może uratować zasoby.

Działalność po fakcie zwykle będzie związana z oszacowaniem szkód i określeniem dlaczego doszło do włamania.

Działalność związana z włamaniem jest związana z podjęciem decyzji czy zezwolić na kontynuację włamania i obserwować intruza, czy wszcząć alarm i prawdopodobnie go spłoszyć. Reakcja może nastąpić dopiero po identyfikacji.

Wykrywanie intruzów

Do podstawowych wymagań stawianych systemom wykrywania intruzów należy:

Ciągła czujność.

Niewidoczność.

Infrastruktura. Monitorowane dane powinny być kontrolowane - przeglądane.

Zmylenie przeciwnika. Przeciwnik powinien uwierzyć, że kontrola jest rzeczywista nawet jeżeli stosujemy jedynie atrapy.

Wykrywanie intruzów

Informacje o monitorowanym systemie przekazywane są w formie raportów.

Infrastruktura zabezpieczeń i ochrony systemu może być wbudowana w jednostkę monitorowania lub stanowić element samodzielny.

Komputery analizujące ruch muszą posiadać wystarczająco wydajne procesory, by były w stanie analizować przechodzący ruch, jak również wykonywać normalne zadania. Od spełnienia tych kryteriów zależy skuteczność całego systemu.

Wiele ataków wykorzystuje bowiem fakt, że maszyna analizująca nie będąc w stanie przejrzeć cały ruch, przepuszcza część ramek, w tym również te zawierające atak.

Kategorie systemów detekcji intruzów

IDS hostowy (Host IDS)

IDS sieciowy (Network IDS),

IDS węzłowy (Network Node IDS).

Kategorie systemów detekcji intruzów

Podstawowe zalety i wady rozwiązań typu **HIDS**:

- Dzięki swojej obecności bezpośrednio na komputerze i stałemu monitorowaniu lokalnych zasobów mogą wykryć ataki niewidoczne dla sieciowych IDS.

- Niezależne od topologii sieciowej.

- Dzięki integracji z systemem operacyjnym mogą skutecznie działać nawet w oparciu o zaszyfrowane dane.

- Mogą wykrywać różne rodzaje "koni trojańskich" lub pewne rodzaje ataków powodujące naruszenie integralności oprogramowania (kasowanie plików etc.).

- Trudne do zarządzania.

- Mogą zostać wyłączone przy użyciu pewnych typów ataków DoS.

- Wymagają dużej przestrzeni dyskowej.

- Obciążające (zmniejszające wydajność) systemu produkcyjnego.

Kategorie systemów detekcji intruzów

NIDS:

Rozwiązania typu NIDS monitorują ruch sieciowy w czasie rzeczywistym, sprawdzając szczegółowo pakiety w celu wykrycia niebezpiecznej zawartości, bądź też rozmaitych typów ataków, zanim osiągną one miejsce przeznaczenia.

Mechanizm działania opiera się na porównywaniu pakietów z sygnaturami ataków (attack signatures), przechowywanymi w bazie danych IDS, lub na analizie użytych protokołów, mającej na celu wyszukiwanie w nich wszelkich anomalii.

Bazy danych sygnatur cały czas uaktualniane są przez dostawców systemów IDS, w miarę wykrywania coraz to nowych form ataków.

Kategorie systemów detekcji intruzów

Zalety i wady rozwiązań typu **NIDS**:

Kilka dobrze umiejscowionych sieciowych systemów wykrywania intruzów może monitorować rozległą sieć.

Rozmieszczenie takich systemów nie wpływa na aktualną topologię sieci.

Systemy NIDS są przeważnie pasywne w swoich działaniach i nasłuchując w danym segmencie nie zakłócają jednocześnie pracy sieci.

Są odporne na ataki, mogą nawet zostać skonfigurowane jako niewidzialne dla potencjalnego włamywacza.

Problemy z analizą wszystkich pakietów w rozległej i ruchliwej sieci.

Kłopoty ze znalezieniem optymalnej lokalizacji.

Brak możliwości analizy zaszyfrowanych danych.

Kategorie systemów detekcji intruzów

Zalety i wady rozwiązań typu **NNIDS**:

Nie zajmują się wszystkimi pakietami krążącymi w sieci co powoduje, iż pracują one znacznie szybciej i wydajniej, co z kolei pozwala na instalowanie ich na istniejących serwerach bez obawy ich przeciążenia.

Niezależne od topologii sieciowej.

Zaszyfrowane dane nie stanowią dla nich przeszkody - dzięki obecności bezpośrednio na komputerze mogą mieć dostęp do danych po ich deszyfracji.

Konieczne jest instalowanie całego szeregu pakietów - po jednym na każdym chronionym komputerze - a każdy z nich musi przekazywać raporty do centralnej konsoli.

Mogą zostać wyłączone w przypadku udanego ataku na komputer.

Zużywają zasoby monitorowanego serwera, co prowadzi zwykle do obniżenia wydajności.

Pułapki internetowe

Internetowa pułapka jest zbiorem elementów funkcjonalnych, które posługują się oszustwem w celu odwrócenia uwagi potencjalnego intruza od rzeczywistych, wartościowych zasobów poprzez użycie zasobów fikcyjnych i skierowanie intruza do systemu gromadzenia informacji wiążących się z włamaniami oraz reagowania.

Zasada działania pułapki

polega na tym, że intruz wchodzi w interakcję ze zbiorem zasobów rzeczywistych, których aktywność jest monitorowana przez system wykrywania włamań. Po uzyskaniu wystarczających dowodów włamania intruz jest kierowany do zasobów fikcyjnych. Działanie wyzwalające pułapkę może być specjalnie oznaczona operacją lub iteracja pewnego zdarzenia, która przekroczy wyznaczoną wartość progową lub dowolny inny symptom włamania.

Cel umieszczenia pułapki

Aby poznać sposób działania intruza oraz dowiedzieć się z jakich technik korzysta. Zdobytą wiedzę można użyć do lepszego zabezpieczenia sieci produkcyjnej.

Zdobyć niepodważalne dowody włamania, które można wykorzystać do zlokalizowania włamywacza oraz w postępowaniu prawnym.

Testy penetracyjne

Co ma na celu test?

- empiryczne określenie odporności systemu na ataki.

Miejsce przeprowadzenia testu?

Testy mogą być prowadzone z wnętrza badanej sieci oraz z zewnątrz.
Testy zewnętrzne są zwykle realizowane przez ludzi, którzy nie znają penetrowanego systemu. Nie znają szczegółów jego topologii konfiguracji i zabezpieczeń.

Test penetracyjny rozpoczyna się zwykle od zebrania informacji o systemie poza nim samym. Może obejmować analizowanie pakietów rozgłoszeniowych, badanie DNS, uzyskiwanie danych u dostawcy usług internetowych przeszukiwanie publicznych zbiorów informacji jak WWW czy LDAP.

Testy penetracyjne

Test penetracyjny wykonywany z zewnątrz może obejmować:

Rekonesans - zbieranie informacji o celu ataku.

Skanowanie przestrzeni adresowej sieci prywatnej - wykrywanie dostępnych serwerów, stacji roboczych, drukarek, routerów i innych urządzeń.

Skanowanie sieci telefonicznej - wykrywanie aktywnych modemów sieci prywatnej.

Skanowanie portów serwerów i urządzeń sieciowych - wykrywanie dostępnych usług.

Identyfikacja systemu - ustalanie rodzaju i wersji systemu, oprogramowania użytkowego, kont użytkowników.

Symulacja włamania - przejmowanie kont, odczytywanie informacji z baz, odczytywanie katalogów współdzielonych, ataki na system kontroli dostępu.

Badanie odporności na ataki typu odmowa usługi (denial of service) - uruchamianie exploitów typu WinNuke, Teardrop, Smurf, Nestea.

Testy penetracyjne

Test penetracyjny wykonywany wewnątrz może obejmować:

podsłuch sieciowy (sniffing),

przechwytywanie połączeń (hijacking).

Metody i techniki rekonesansu

Jakie informacje można uzyskać w wyniku rekonesansu?

nazwę domeny,

bloki sieci,

adresy IP komputerów osiągalnych poprzez usługi działające na zidentyfikowanych komputerach,

architekturę i zainstalowany system operacyjny,

mechanizmy kontroli dostępu,

systemy wykrywania intruzów i zapory sieciowe,

używane protokoły,

numery linii telefonicznych,

mechanizmy autoryzacji dla zdalnego dostępu.

Metody i techniki rekonesansu

Gdzie można uzyskać informację?

- ogólnie dostępne źródła, np:

    - strony www,
    - artykuły i informacje prasowe,
    - listy dyskusyjne,
    - serwisy wyszukiwawcze.

- komentarze w kodzie źródłowym strony www.

    - informacje o lokalizacji,
    - powiązane firmy i jednostki organizacyjne,
    - informacje o przejęciach i fuzjach,
    - numery telefonów,
    - adresy kontaktowe i adresy e-mail,
    - informacje o polityce prywatności i zabezpieczeń,
    - łącza do innych serwerów powiązanych z organizacją.

Metody i techniki rekonesansu

Gdzie można uzyskać informację?

- bazy danych **whois**

www.allwhois.com
www.arin.net - American Registry for Internet Numbers
www.samspade.org – SamSpade
ww.dns.pl - Naukowa i Akademicka Sieć Komputero

- kontrola serwerów DNS (umożliwienie nieautoryzowanym użytkownikom na dokonanie przesłania strefy serwera DNS; *nslookup*)

- badanie sieci (*traceroute* (UNIX) lub *tracert* (Windows))

-skanowanie ICMP / TCP / UDP

- mapowanie odwrotne - metoda wykrywania komputerów funkcjonujących w sieci może być wysyłanie pakietów z ustawioną flagą RST, tzw. inverse mapping. Metoda ta wykorzystywana jest z reguły do poznania topologii sieci - stwierdzenia, czy dany komputer istnieje czy nie.

Techniki skanowania

Skanowanie ICMP

Najprostsza, najczęściej stosowana ale i coraz mniej skuteczną metoda.

Polega na wysłaniu pakietu ICMP echo request (ping).

Na tej podstawie można stwierdzić czy docelowe urządzenie jest osiągalne.

Brak odpowiedzi nie świadczy jednak o tym, że komputer nie jest nieosiągalny.

Powodów braku odpowiedzi może być wiele: zapora ogniowa filtrująca pakiety ICMP, wyłączony serwis na docelowym komputerze i wiele innych.

Techniki skanowania

Skanowanie TCP

Pewne cechy protokołu TCP sprawiają, że jest on bardziej przydatny do skanowania niż np. protokół UDP.

W skanowaniu ważne może być również śledzenie numerów sekwencyjnych oraz odpowiedzi systemu po otrzymaniu pakietu TCP z włączonymi określonymi flagami.

Z reguły stosowane są pakiety nie zawierające danych, gdyż ważny jest fakt, czy zdalny system odpowiedział, a nie zawartość pola danych pakietu.

Pewne techniki wykorzystują fragmentację pakietów w warstwie sieciowej, które pozwalają ukryć nagłówek TCP w kilku pakietach IP utrudniając detekcję skanowania.

Techniki skanowania

Skanowanie UDP

W przypadku bezpołączeniowego protokołu UDP reakcja zdalnego systemu może być dwojaka. Aktywny system w momencie otrzymania datagramu UDP na zamknięty port powinien wysłać komunikat ICMP Port Unreachable.

W przeciwnym przypadku, gdy port jest otwarty, nie należy się spodziewać odpowiedzi, gdyż w przypadku UDP nie występuje potwierdzanie odebrania pakietu.

Czasami można uzyskać odpowiedź z portu otwartego, gdy serwer usługi ulokowanej w tym porcie próbuje odpowiedzieć na domniemane żądanie.

Zależeć to będzie przede wszystkim od sposobu budowania pakietu skanującego.