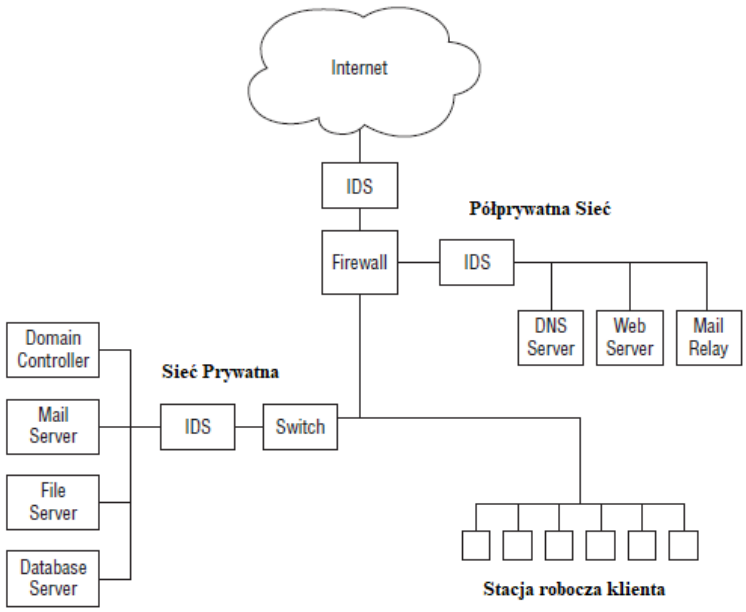
Systemy wykrywania włamań (IDS), firewalle i honeypoty to wszystkie środki bezpieczeństwa stosowane w celu zapewnienia, że haker nie będzie w stanie uzyskać dostępu do sieci lub systemu docelowego. IDS i zapora ogniowa są zasadniczo urządzeniami filtrującymi pakiety i służą do monitorowania ruchu w oparciu o wstępnie zdefiniowany zestaw reguł. Honeokot to fałszywy system docelowy używany do odciągania hakerów od bardziej wartościowych celów. Podobnie jak w przypadku innych mechanizmów bezpieczeństwa, IDS, firewall i honeypots są tak dobre, jak ich projektowanie i implementacja. Ważne jest, aby zapoznać się z działaniem tych urządzeń i zapewnić bezpieczeństwo, ponieważ są one często przedmiotem ataku.

Rodzaje IDS i techniki unikania

Systemy wykrywania włamań (IDS) kontrolują ruch i szukają znanych sygnatur ataków lub nietypowych wzorców zachowań. Widok sniffera pakietów monitoruje ruch i jest wbudowanym komponentem IDS. IDS ostrzega centrum dowodzenia lub administratora systemu przez pager, e-mail lub telefon komórkowy, gdy zostanie wyzwolone zdarzenie pojawiające się na liście zdarzeń bezpieczeństwa firmy. Systemy zapobiegania włamaniom (IPS) inicjują środki zaradcze, takie jak blokowanie ruchu w przypadku wykrycia podejrzanego przepływu ruchu. IPS automatyzują reakcję na próbę włamania i umożliwiają automatyzację możliwości odmowy dostępu. Istnieją dwa główne typy IDS:

Host-based Hosts IDS (HIDS) to aplikacje rezydujące na jednym systemie lub hoście i filtrujące ruch lub zdarzenia na podstawie listy znanych sygnatur dla tego konkretnego systemu operacyjnego. HIDS to Norton Internet Security i Cisco Security Agent (CSA). Wiele robaków i trojanów może wyłączyć HIDS. HIDS można również instalować bezpośrednio na serwerach w celu wykrywania ataków na zasoby i aplikacje korporacyjne.

Sieciowe identyfikatory IDS (NIDS) oparte na sieci są urządzeniami programowymi, które znajdują się w sieci. Są używane wyłącznie do wykrywania włamań w celu wykrycia wszelkiego rodzaju złośliwego ruchu sieciowego i użycia komputera, którego nie można wykryć za pomocą standardowej zapory. Obejmuje to ataki sieciowe na wrażliwe usługi; ataki danych na aplikacje; ataki oparte na hostach, takie jak eskalacja uprawnień, nieautoryzowane logowanie i dostęp do poufnych plików; i złośliwe oprogramowanie. NIDS są systemami pasywnymi: czujnik IDS wykrywa potencjalne naruszenie bezpieczeństwa, rejestruje informacje i sygnalizuje alarm na konsoli. Lokalizacja IDS w sieci w architekturze sieci została przedstawiona na rysunku



Czujnik IDS sieci może być zlokalizowany jako pierwszy punkt detekcji między zaporą ogniową a Internetem lub na półprywatnym DMZ, wykrywając ataki na serwery organizacji. Wreszcie, IDS sieci może znajdować się w wewnętrznej sieci prywatnej, a serwery korporacyjne wykrywają możliwe ataki na te serwery. IDS może wykonać analizę sygnatur lub wykrywanie anomalii, aby określić, czy ruch to możliwy atak. Identyfikatory wykrywania podpisów dopasowują ruch do znanych sygnatur i wzorców niewłaściwego użycia. Sygnatura jest wzorcem służącym do identyfikacji pojedynczego pakietu lub serii pakietów, które po połączeniu przeprowadzają atak. IDS, który wykorzystuje wykrywanie anomalii, szuka prób włamań w oparciu o normalne wzorce biznesowe danej osoby i ostrzega, gdy wystąpi anomalia w zachowaniu dostępu do systemów, plików, logowań i tak dalej. Haker może uniknąć IDS, zmieniając ruch tak, aby nie pasował do znanego podpisu. Może to wymagać użycia innego protokołu, takiego jak UDP zamiast TCP lub HTTP zamiast protokołu ICMP w celu przeprowadzenia ataku. Dodatkowo, haker może przebić atak na kilka mniejszych pakietów, aby przejść przez IDS, ale po ponownym złożeniu w stacji odbiorczej, doprowadzi to do kompromisu systemu. Jest to tak zwane splatanie sesji. Inne metody unikania wykrycia obejmują wstawianie dodatkowych danych, zaciemnianie adresów lub danych za pomocą szyfrowania lub desynchronizowania i przejmowania bieżącej sesji klienta.

Narzędzie hakerskie

ADMmutate przyjmuje skrypt ataku i tworzy inny, ale funkcjonalnie równoważny skrypt do wykonania ataku. Nowy skrypt nie znajduje się w bazie znanych sygnatur ataków i dlatego może ominąć IDS.

Zrozumienie reguł i wyników Snort

Jako etyczny haker powinieneś zapoznać się z zasadami Snorta i jego wynikami. Może zajść potrzeba przeczytania reguły Snort lub wyjścia i odpowiedzi na pytanie dotyczące tego, co robi reguła lub jaki rodzaj ataku jest wskazywany przez dane wyjściowe. Snort to sniffer pakietów w czasie rzeczywistym, HIDS i narzędzie do rejestrowania ruchu wdrożone w systemach Linux i Windows. Snort może analizować protokoły, wyszukiwać i dopasowywać zawartość oraz wykrywać różnorodne ataki i sondowanie, takie jak przepełnienia bufora, skanowanie portów, ataki CGI, sondy SMB, próby pobierania odcisków palców systemu operacyjnego i wiele innych. Możesz skonfigurować Snort i reguły IDS w pliku snort.conf. Polecenie instalacji i uruchamiania Snorta to:

snort -l c: \ snort \ log -c C: \ snort \ etc \ snort.conf -A console

Snort składa się z dwóch głównych komponentów:

Snort Engine. Mechanizm wykrywania IDS, który wykorzystuje modułową architekturę wtyczek

Reguły Snorta. Elastyczny język reguł do opisu ruchu, który ma zostać zebrany

Snort Engine jest dystrybuowany zarówno jako kod źródłowy, jak i pliki binarne dla popularnych dystrybucji Linux i Windows. Należy zauważyć, że zasady Snort Engine i Snort są dystrybuowane osobno. Snort IDS Engine i zasady można pobrać ze strony snort.org. Metody instalacji i zależności oprogramowania różnią się w zależności od systemu operacyjnego, dlatego ten rozdział nie obejmuje laboratorium instalowania Snort. Szczegółowe instrukcje instalacji można znaleźć na stronie snort.org.

Konfigurowanie Snort

Snort ma jeden plik konfiguracyjny: snort.conf. Zwykle znajduje się w / etc / snort. Plik zawiera zmienne, które należy zmodyfikować dla konkretnej instalacji i dostosowane do zdarzeń, które chcesz ostrzec. Zmienne pliku są uporządkowane w następujących sekcjach:

* Zmienne sieciowe

* Preprocesory

* Postprocesory

* Reguły

Zmienne sieciowe pliku snort.conf, które należy dostosować do twojej sieci, są wymienione w tabeli

Zmienne	Znaczenie
HOME_NET	Lokalna przestrzeń adresów IP
EXTERNAL_NET	Zewnętrzna przestrzeń adresowa IP
SMTP	Twoje serwery SMTP
HTTP_SERVERS	Twoje serwery internetowe
SQL_SERVERS	Twoje serwery SQL
DNS_SERVERS	Twoje serwery DNS
RULE_PATH	Katalog zawierający twoje pliki reguł

Oto przykładowy plik konfiguracyjny Snorta wykorzystujący sieć 192.168.1.0 jako sieć domowa:

```
var HOME_NET 192.168.1.0/24
var EXTERNAL_NET any
var SMTP $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var DNS_SERVERS $HOME_NET
var RULE_PATH /etc/snort/rules
```

Poniżej znajdują się lokalizacje reguł określone w pliku konfiguracyjnym:

```
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
```

include $RULE_PATH/web-cgi.rules

include $RULE_PATH/web-coldfusion.rules

include $RULE_PATH/web-iis.rules

include $RULE_PATH/web-frontpage.rules

include $RULE_PATH/web-misc.rules

include $RULE_PATH/web-attacks.rules

include $RULE_PATH/sql.rules

include $RULE_PATH/netbios.rules

include $RULE_PATH/misc.rules

Zasady Snort

Reguły snortowe służą do generowania alertów na podstawie ruchu, który jest wyświetlany przez mechanizm przetwarzania IDS. Wszystkie reguły mają nagłówek reguły złożony z następujących pól:

* <akcja reguły>

* <protokół>

* <adres src i port>

* <adres docelowy i port>

Oto przykład reguły Snort:

alert tcp $ EXTERNAL_NET any -> $ HOME_NET 23

Ta reguła mówi, aby wygenerować alert (i komunikat dziennika) dla dowolnego pakietu TCP pochodzącego z zewnętrznej przestrzeni adresowej (i dowolnego portu) przeznaczonej dla lokalnej przestrzeni adresowej (i portu 23). Po nagłówku reguły Snorta następują opcje reguł, które są rozdzielaną listą funkcji używanych w Snort. Oto niektóre opcje reguł i objaśnienia. Linia

msg: "Błąd formatu telnetd TELNET SGI"

określa do rejestrowania i ostrzegania silników, jaki komunikat do wydrukowania. Linia

flagi: A +

dopasowuje flagę TCP ACK (i dowolną inną flagę zestawu). Linia

treść: "bin / sh"

dopasowuje podany ciąg w pakiecie ładunku. Linia

classtype: attempted-admin

przypisuje wysoki priorytet temu alertowi, nadając mu klasę ataku usiłowanego administratora (próba zwiększenia uprawnień administratora).

Dane wyjściowe Snort

W przypadku etycznego hakera ważne jest zrozumienie raportu wyjściowego Snort. Oto przykład alertu Snort. Najpierw tutaj jest znacznik czasu:

04 / 21-19: 26: 37,353790

Są to źródłowe i docelowe adresy MAC:

0: 8: 2: FB: 36: C6 -> 0: 6: 5B: 57: A6: 3F

Typ ramki Ethernet (0x800 oznacza Ethernet) i długość są następujące:

typ: 0x800 len: 0x3C

Ten wiersz określa źródłowy adres IP 202.185.44.43 na docelowy adres IP 202.185.44.28 i port źródłowy 445 oraz port docelowy 2202:

202.185.44.43:445 -> 202.185.44.28:2202

Ten wiersz stwierdza, że protokół to TCP, a Time To Live (TTL) to 128:

TCP TTL: 128

Dalej jest typ usługi, identyfikator, długość IP i długość datagramu:

TOS: 0x0 ID: 17467 IpLen: 20 DgmLen: 41 DF

*** A **** oznacza, że flaga ACK jest włączona, więc pakiet jest potwierdzeniem poprzedniego pakietu:

ZA*

W tym wierszu Seq jest numerem kolejnym, a Ack jest numerowaną odpowiedzią na poprzedni pakiet:

Seq: 0x9D08DD67 Ack: 0x83EB1E02

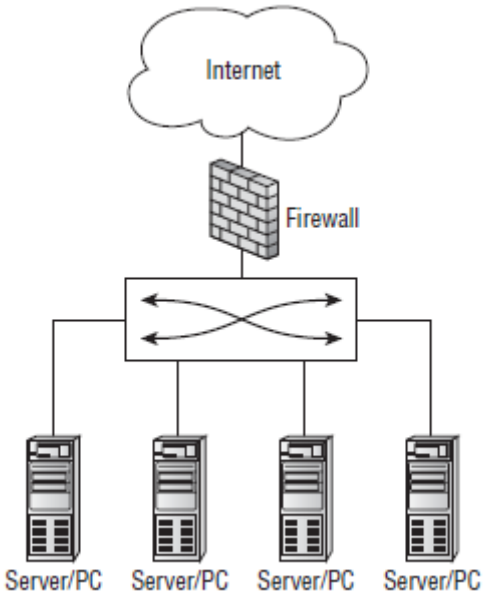
Wreszcie, w następującym wierszu Win to rozmiar okna, a długość TCP to 2000:

Wygraj: 0x3FE1 TcpLen: 2000

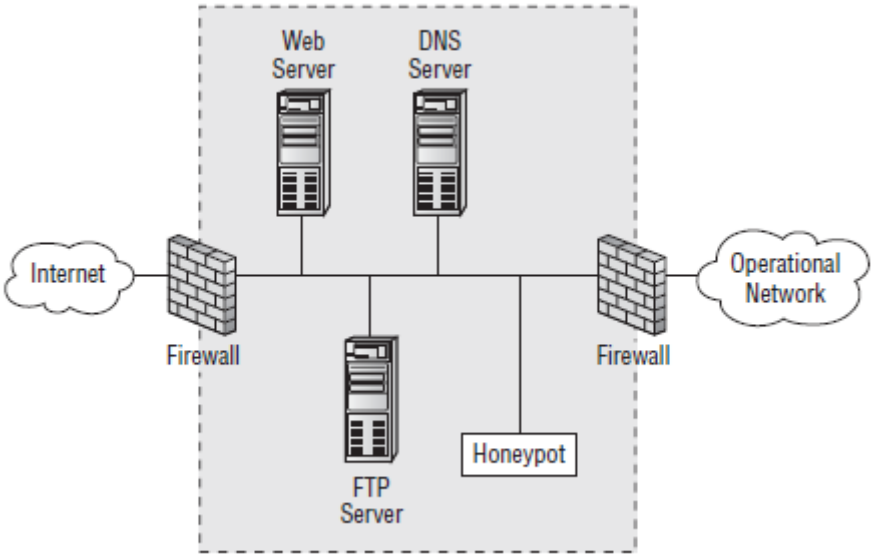
W wielu przypadkach czytanie i interpretacja raportów wyjściowych Snorta na egzaminie CEH jest tylko kwestią znajomości flag TCP i dobrze znanych numerów portów TCP.

Typy firewalli i techniki unikania honeypot

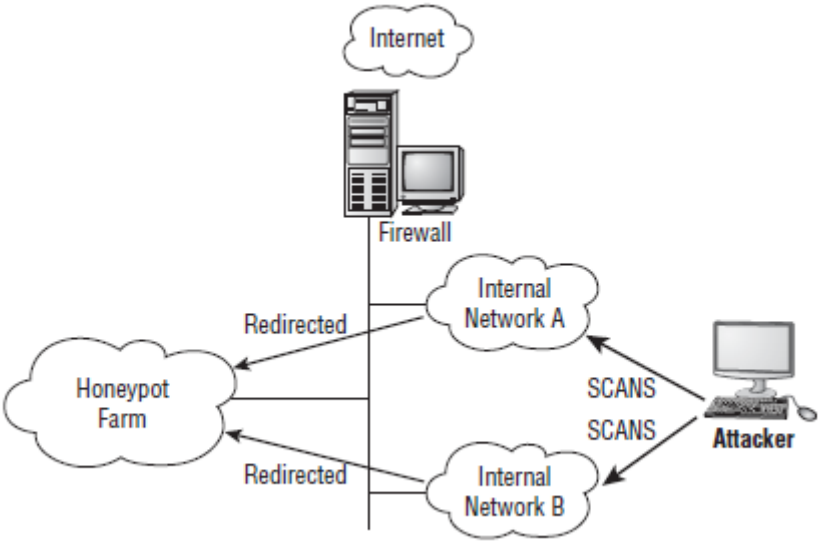
Zapora ogniowa to program lub urządzenie sprzętowe, które zezwala lub odmawia dostępu do sieci i postępuje zgodnie z regułami ustalonymi przez administratora w celu wskazania, gdzie pakiety mogą być przesyłane w sieci. Obwód sprzętowej zapory ogniowej



jest ustawiony na krawędzi sieci, gdzie zaufana sieć łączy się z niezaufaną siecią, taką jak Internet lub między sieciami. Zapora programowa chroni komputer osobisty, system lub host przed niepożądanymi lub złośliwymi pakietami wchodzącymi z karty sieciowej (NIC) z sieci. Honeypot



to pułapka z wabikami znajdujące się wewnątrz strefy zdemilitaryzowanej sieci (DMZ), skonfigurowane przez specjalistę od zabezpieczeń do łapania w pułapkę lub pomocy w lokalizowaniu hakerów lub odciągnięcia ich od prawdziwego systemu docelowego. Honeypot to system wabików, który złośliwy atakujący może spróbować zaatakować; oprogramowanie w systemie może rejestrować informacje o atakującym, takie jak adres IP. Informacji tej można użyć, aby zlokalizować atakującego podczas lub po ataku. Najlepsze miejsce dla honeypota znajduje się przed firewallem na DMZ, co czyni go atrakcyjnym dla hakerów. Honeypot o statycznym adresie ma wyglądać jak prawdziwy serwer produkcyjny



Ćwiczenie 13.1 przeprowadzi cię przez instalację i używanie honeypota

Znajdowanie Honeypot'a

Przeprowadziłem audyt bezpieczeństwa sieci bezprzewodowej dla dużej korporacji sprzed kilku lat. Jeździłem po korporacyjnym kampusie, szukając otwartych punktów dostępowych (AP), i byłem nieco zaskoczony, jak wiele otwartych niezabezpieczonych punktów dostępowych może być widzianych przez mój bezprzewodowy skaner sniffujący. Znalazłem ponad 30 punktów dostępu, do których mogłem się podłączyć i uzyskać dostęp do sieci. Oczywiście następnym krokiem po podłączeniu do AP było przeskanowanie sieci. W ramach audytu bezpieczeństwa połączyłem się z zewnątrz budynku i przeprowadziłem skanowanie portów w całym zakresie sieci; Znalazłem kilka systemów z otwartymi portami. Był serwer pocztowy i kilka serwerów internetowych, a także kontroler domeny, który nie był całkowicie załatany. Zgodnie z zakresem audytu miałem tylko zgłosić wykryte luki i nie próbować wykorzystywać usług, które znalazłem działające w systemach. Byłem zaskoczony, że tak duża organizacja będzie miała luki tak łatwo wykryte w otwartej sieci bezprzewodowej. Udokumentowałem wszystkie systemy docelowe i wrażliwe porty i usługi w moim raporcie kontroli bezpieczeństwa. Kiedy przedstawiłem mój raport klientowi następnego dnia, kierownik IT po prostu powiedział: "Dobrze, znalazłeś naszą honeynet, teraz idź znaleźć prawdziwe systemy." Zabrali wszystkie nieuczciwe punkty AP odkryte w sieci i przetransportowali je do oddzielnej sieci VLAN. Następnie na zablokowanej sieci VLAN stworzyli fałszywe systemy lub honeypoty, aby przyciągnąć potencjalnych hakerów. Te honeypoty mogą powstrzymać hakera przed atakowaniem systemu honeypot bez rzeczywistych danych, podczas gdy prawdziwe usługi pozostają nietknięte.

Ćwiczenie 13.1

Instalowanie i używanie KFSensor jako Honeypot

1. Pobierz i zainstaluj wersję próbną KFSensor ze strony www.keyfocus.net.

2. Otwórz i uruchom KFSensor. Pojawi się wyskakujące okno, aby uruchomić kreatora konfiguracji. Naciśnij dalej by kontynuować.

3. Kliknij Dalej, aby wybrać wszystkie porty.

4. Wpisz swoją nazwę.com (lub inną wybraną nazwę domeny) w domenie Nazwa pola i kliknij Dalej.

5. Wpisz swój adres e-mail w polach Wyślij do i Wyślij od, aby otrzymywać powiadomienia e-mail z KFSensor.

6. Z listy rozwijanej Aktywność portu wybierz 8 godzin. Wybierz opcję Włącz pliki zrzutu pakietów z rozwijanego menu Network Protocol Analyzer. Inne opcje mogą pozostać domyślne.

7. Kliknij przycisk Dalej, aby zaakceptować ustawienie domyślne, aby zainstalować jako usługę systemową.

8. Kliknij przycisk Zakończ, aby ukończyć konfigurację kreatora.

9. Główny scenariusz dla KFSensor powinien pojawić się po lewej stronie. Może pojawić się komunikat wskazujący, że niektóre porty zostały wyłączone, ponieważ są używane przez usługi systemowe; tekst przekierowania wskazuje, że porty nie są dostępne w KFSensor. Wykonaj skanowanie portu w stosunku do systemu, w którym działa KFSensor, aby zidentyfikować usługi.

10. Spróbuj połączyć się z działającą usługą

11. Wyświetl odwiedzającego do HBSypot KFSensor, klikając menu Widok i wybierając Użytkownicy.

12. Kliknij adres IP odwiedzającego, aby wyświetlić połączenia.

13. KFSensor będzie działał nawet po zamknięciu programu. Aby całkowicie zatrzymać serwery, kliknij prawym przyciskiem myszy ikonę KFSensor na pasku zadań i wybierz Zatrzymaj serwer. Na systemie KFSensor.

Najprostszym sposobem na ominięcie zapory jest złamanie zabezpieczeń systemu po zaufanej lub wewnętrznej stronie zapory. Zaatakowany system może następnie połączyć się poprzez firewall, z zaufanego do niezaufanego boku, z systemem hakera. Powszechną metodą jest to, aby skompromitowany system łączył się z hakerem z portem docelowym 80, który wygląda jak klient sieciowy łączący się z serwerem WWW przez zaporę ogniową. Jest to określane jako odwrotna powłoka WWW. Atak ten działa, ponieważ większość zapór ogniowych zezwala domyślnie na wychodzące połączenia do portu 80. Wykorzystując tunel do wysyłania ruchu HTTP, haker omija zaporę ogniową i sprawia, że atak wygląda nieszkodliwie na zaporę; takie ataki są praktycznie niemożliwe do wykrycia przez administratorów systemu. Programy hakerskie mogą tworzyć ukryte kanały, które pozwalają atakować ruch w dół na dozwoloną ścieżkę, taką jak żądanie lub odpowiedź ping ICMP (Internet Control Message Protocol). Inna metoda wykorzystania ukrytego kanału tuneluje ruch ataku jako potwierdzenie TCP. Aby uniknąć pułapki zastawionej przez honeypota, haker może uruchomić oprogramowanie anty-honeypot, które próbuje ustalić, czy honeypot działa w systemie docelowym i ostrzega go przed hakerem. W ten sposób haker może próbować uniknąć wykrycia, nie atakując honeypota. Większość programów antywirusowych sprawdza oprogramowanie uruchomione w systemie przed znaną listą honeypotów, takich jak honeyd.

Narzędzia hakerskie

007 Shell to program tunelujący powłoki, który pozwala hakerowi używać ukrytego kanału dla ataku, a tym samym ominąć reguły zapory ogniowej.

ICMP Shell to program podobny do telnetu, który haker wykorzystuje do nawiązania połączenia z systemem docelowym za pomocą tylko poleceń ICMP, które są zwykle dozwolone przez zaporę ogniową.

AckCmd to program klient / serwer komunikujący się przy użyciu tylko pakietów TCP ACK, które zwykle mogą przejść przez zaporę ogniową.

Covert TCP to program, którego haker używa do wysyłania pliku przez zaporę po jednym bajcie na raz, ukrywając dane w nagłówku IP.

Send-Safe Honeypot Hunter to narzędzie do wykrywania honeypot, które sprawdza się przed serwerem proxy dla honeypotów.

Środki zaradcze

Spectre to system typu honeypot, który automatycznie rejestruje informacje o komputerze hakera podczas ataku na system. Honeyd to honeypot typu open source, który tworzy wirtualne hosty w sieci, która jest następnie atakowana przez hakerów.

KFSensor to IDS oparty na hoście, który działa jako honeypot i może symulować wirtualne usługi i instalacje trojanów. Sobek to narzędzie honeypot do przechwytywania danych, które przechwytuje sekwencję klawiszy atakującego. Skaner narażenia na atak Nessus (www.nessus.org) może być również używany do wykrywania honeypotów.

Podsumowanie

Systemy wykrywania włamań mogą być oparte na sieci lub na hoście. Ważne jest, aby zaimplementować oba typy w celu ochrony cennych danych na serwerach przed atakami. W obu przypadkach ważne jest, aby zasady i definicje były aktualne, aby zapewnić IDS najnowsze ataki w celu porównywania ruchu. Zapory mogą również być oparte na sieci lub hostach, a w wielu przypadkach oprogramowanie urządzeń sieciowych i systemów wykonuje zarówno wykrywanie IDS, jak i działania zapory ogniowej. Tylko dlatego, że firewall i IDS są zaimplementowane w sieci lub serwerze, nie powinieneś uśpić fałszywego poczucia bezpieczeństwa; tunelowanie i szyfrowanie mogą zniszczyć zarówno IDS, jak i zapory, ponieważ rzeczywiste nagłówki ruchu i dane nie mogą być odczytane przez urządzenie. CEH korzysta z takich technik, próbując ominąć ochronę zapór ogniowych i IDS.

Do Zapamiętania !

* Poznałeś dwa główne typy IDS. IDS mogą być oparte na hoście lub na sieci. IDS oparty na hostach jest specyficzny dla systemu operacyjnego i chroni jeden system. Identyfikator sieciowy może chronić całą sieć.

* Zdefiniowałeś honeypot. Honeypot znajduje się w strefie DMZ jako podatny host i reklamuje usługi i oprogramowanie, które zachęcają hakerów do włamywania się do systemu.

* Zdefiniowałeś zaporę ogniową. Zapora ogniowa to urządzenie filtrujące pakiety, które porównuje ruch z listą reguł i filtruje ruch z niezaufanej sieci do zaufanej sieci.

* Dowiedziałeś się, jak wykryć honeypot. Można wykryć honeypot porównując informacje o systemie do znanej listy honeypotów na serwerze proxy.

* Dowiedziałeś się, jak działa IDS. IDS może przeprowadzić analizę anomalii lub wykrywanie oparte na sygnaturach.

* Dowiedziałeś się, jak wykonywać techniki unikania zapory ogniowej. Zapobieganie zaporom można wykonać za pomocą protokołu, takiego jak ICMP lub HTTP, aby przenosić ruch ataków. Inną techniką jest dzielenie pakietów na kilka mniejszych pakietów, więc cały ciąg ataków nie może zostać wykryty.