Sniffer to narzędzie przechwytywania pakietów lub przechwytywania klatek. Zasadniczo przechwytuje i wyświetla dane podczas przesyłania z hosta do hosta w sieci. Zwykle sniffer przechwytuje ruch w sieci i wyświetla go w postaci wiersza poleceń lub formatu GUI dla hakera do obejrzenia. Większość snifferów wyświetla nagłówek warstwy 2 (ramka) lub warstwy 3 (pakiet) i ładunek danych. Niektóre wyrafinowane sniffery interpretują pakiety i mogą ponownie połączyć strumień pakietów z oryginalnymi danymi, takimi jak e-mail lub dokument. Sniffery są używane do przechwytywania ruchu przesyłanego między dwoma systemami, ale mogą również dostarczać wiele innych informacji. W zależności od sposobu użycia sniffera i zastosowanych zabezpieczeń haker może użyć sniffera do wykrycia nazw użytkowników, haseł i innych poufnych informacji przesyłanych w sieci. Kilka ataków hakerskich i różnych narzędzi hakerskich wymaga użycia sniffera w celu uzyskania ważnych informacji wysłanych z systemu docelowego. Tu opisujemy, jak działają sniffery i identyfikujemy najczęstsze narzędzia hakerskie do snifferów.

Termin pakiet odnosi się do danych w warstwie 3 lub w warstwie sieciowej modelu OSI, podczas gdy ramka odnosi się do danych w warstwie 2 lub warstwie łącza danych. Ramki zawierają adresy MAC, a pakiety zawierają adresy IP.

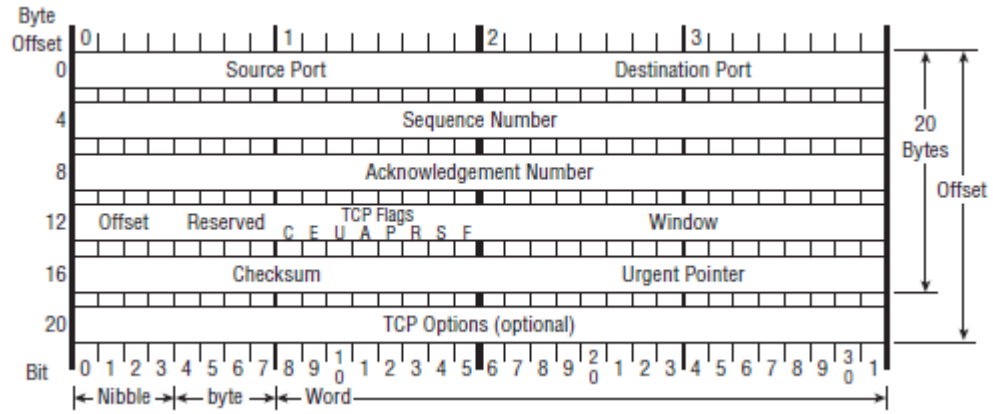
Omówienie komunikacji Host-Host

Cała komunikacja sieciowa Host-to-Host oparta jest na modelu komunikacji danych TCP / IP. Model TCP / IP jest modelem czterowarstwowym. Model TCP / IP odwzorowuje starszy model OSI z 7 warstwami komunikacji danych. Większość aplikacji wykorzystuje pakiet TCP / IP do przesyłania danych między hostami.

Model OSI	Model TCP/IP (Model DoD)
Aplikacja	
Preszentacja	Aplikacja
Sesja	
Transport	Transport
Sieć	Internet
Łącze danych	
Fizyczna	Dostęp do Sieci

W normalnych operacjach sieciowych dane warstwy aplikacji są enkapsulowane, a nagłówek informacji o adresie jest dodawany na początku danych. Nagłówek IP zawierający źródłowy i docelowy adres IP są dodawane do danych, jak również nagłówek MAC zawierający źródłowe i docelowe adresy MAC. Adresy IP są używane do kierowania ruchu do odpowiedniej sieci IP, a adresy MAC zapewniają, że dane są wysyłane do właściwego hosta w docelowej sieci IP. W ten sposób ruch jest przesyłany z hosta źródłowego do hosta docelowego w Internecie i zapewniane jest dostarczanie do odpowiedniego hosta. System pocztowy działa w podobny sposób. Poczta jest kierowana do odpowiedniego obszaru za pomocą kodu pocztowego, a następnie poczta jest dostarczana w postaci kodu pocztowego na numer domu i ulicy. Adres IP jest podobny do kodu pocztowego, aby dostarczyć pocztę do regionu, a numery ulic i domów są jak adres MAC tej dokładnej stacji w sieci. System adresowy zapewnia dokładną dostawę do odbiorcy. W normalnych operacjach sieciowych host nie powinien odbierać danych przeznaczonych dla innego hosta, ponieważ pakiet danych powinien być odbierany tylko przez zamierzonego odbiorcę. Mówiąc prosto, dane powinny być odbierane tylko przez stację z

prawidłowym adresem IP i MAC. Wiemy jednak, że sniffery otrzymują dane, które nie są dla nich przeznaczone. Co robi poczta z hackowaniem? W realnym świecie czasami poczta nie jest dostarczana do docelowego odbiorcy. Jestem pewien, że wszyscy otworzyliście skrzynkę pocztową, aby odkryć kopertę zaadresowaną do sąsiada lub kogoś, kto mieszkał pod waszym adresem. Zdarza się to dość regularnie w moim domu. Większość osób po prostu pozostawi pocztę w pudełku, aby listonosz mógł ponownie dostarczyć lub fizycznie przekazać kopertę sąsiadowi. Ten sam rodzaj sytuacji może wystąpić w sieciach komputerowych, w których dane warstwy aplikacji nie docierają do zamierzonego adresata z powodu błędu dostarczenia lub innego błędu sieci. Inną przyczyną nieotrzymania poczty przez zamierzonego odbiorcę jest to, że ktoś przeprowadza rekonesans i obserwuje twoją skrzynkę pocztową. Załóżmy, że nie ma Cię w domu, a operator pocztowy dostarcza pocztę do skrzynki pocztowej. Ktoś, kto ogląda skrzynkę pocztową z ulicy lub pobliskiego budynku, może poczekać, aż poczta zostanie dostarczona do skrzynki pocztowej, a oni wyjmą pocztę lub tylko określoną kopertę po wyjęciu z pudełka. Byłoby to szczególnie skuteczne, gdyby haker dokonał rekonesansu i wiedział, o której godzinie każdego dnia dostarczono pocztę. Haker mógł wtedy sprawdzić i przeczytać informacje w kopercie, a jeśli próbowałby ukryć swoje ślady, po prostu zamknął kopertę i umieścił ją z powrotem w skrzynce pocztowej. Sniffowanie danych w sieci odbywa się w podobny sposób. Dane są przechwytywane, czytane i wysyłane do zamierzonego odbiorcy lub po prostu odrzucane. Oprócz zrozumienia adresów sieciowych ważne jest również zrozumienie formatu nagłówka TCP. Rysunek poniższy pokazuje format nagłówka TCP.



Nagłówek TCP składa się z następujących pól:

Port źródłowy: 16 bitów Numer portu źródłowego.

Port docelowy: 16 bitów Docelowy numer portu.

Numer sekwencji: 32 bitowy numer kolejny pierwszego oktetu danych w tym segmencie (z wyjątkiem sytuacji, gdy obecny jest SYN). Jeśli występuje SYN, numer sekwencji jest początkowym numerem sekwencji (ISN), a pierwszy oktet danych to ISN + 1.

Numer potwierdzenia: 32 bity Jeśli ustawiony jest bit kontrolny ACK, to pole zawiera znak wartości następnego numeru sekwencyjnego, którego nadawca oczekuje na otrzymanie.

Przesunięcie danych: 4 bity Liczba 32-bitowych słów w nagłówku TCP. Wskazuje, gdzie zaczynają się dane.

Zarezerwowane: 6 bitów Zarezerwowane do wykorzystania w przyszłości. Musi wynosić zero.

Kontrolne bity: 6 bitów :

* URG: Znaczące pole wskaźnika pilnego

* ACK: Znaczące pole potwierdzenia

* PSH: Funkcja Push

* RST: Zresetuj połączenie

*SYN: Synchronizuj numery sekwencji

* FIN: brak danych od nadawcy

Window: 16 bitów Liczba oktetów danych zaczynająca się od podanej w polu potwierdzenia, które nadawca tego segmentu jest gotów zaakceptować.

Suma kontrolna: 16 bitów Pole sumy kontrolnej to obliczenie wszystkich pól w celu zapewnienia, że wszystkie dane zostały odebrane, a dane nie zostały zmodyfikowane podczas przesyłania.

Wskaźnik pilny: 16 bitów To pole informuje o bieżącej wartości wskaźnika pilnego jako dodatnie przesunięcie od numeru kolejnego w tym segmencie. Wskaźnik pilny wskazuje na numer sekwencji oktetu w następstwie pilnych danych. To pole jest interpretowane tylko w segmentach z ustawionym bitem kontrolnym URG.

Opcje: zmienna Opcje mogą zajmować miejsce na końcu nagłówka TCP i mają wielokrotność 8-bitowych długości.

Odnosząc się do długości pól w nagłówku TCP, 8 bitów zawiera jeden bajt. Nibble to mniej niż bajt, a słowo to więcej niż bajt. W następnej sekcji dowiemy się, jak narzędzie hakerskie manipuluje normalną operacjąw sieci w celu przechwytywania ruchu na hoście, który nie jest zamierzonym odbiorcą.

Jak działa Sniffer

Oprogramowanie Sniffer działa poprzez przechwytywanie pakietów nieprzeznaczonych dla adresu MAC systemu sniffera, ale raczej dla docelowego adresu MAC. Jest to tak zwany tryb promiscuous. Zwykle system w sieci odczytuje i odpowiada tylko na ruch przesyłany bezpośrednio na jego adres MAC. Jednak wiele narzędzi hakerskich zmienia NIC systemu na tryb swobodny. W trybie mieszanym, karta sieciowa odczytuje cały ruch i wysyła go do sniffera w celu przetworzenia. Tryb promiscuous jest włączony na karcie sieciowej z instalacją specjalnego oprogramowania sterownika. Wiele narzędzi hakerskich do podsłuchiwania obejmuje sterownik typu promiscuous, który ułatwia ten proces. Nie wszystkie sterowniki systemu Windows obsługują tryb mieszany, więc podczas korzystania z narzędzi hakerskich upewnij się, że sterownik obsługuje wymagany tryb. Wszelkie protokoły, które nie szyfrują danych, są podatne na podsłuchiwanie. Protokoły takie jak HTTP, POP3, Simple Network Management Protocol (SNMP) i FTP są najczęściej przechwytywane przy użyciu sniffera i przeglądane przez hakera w celu gromadzenia cennych informacji, takich jak nazwy użytkowników i hasła. Istnieją dwa różne rodzaje sniffowania : pasywne i aktywne. Pasywne sniffowanie obejmuje słuchanie i przechwytywanie ruchu, i jest użyteczne w sieci połączonej z koncentratorami; Aktywne sniffowanie polega na uruchomianiu fałszowania protokołu ARP (ang. Address Resolution Protocol) lub ataku polegającego na zatłoczeniu ruchu w stosunku do przełącznika w celu przechwytywania ruchu. Jak wskazują nazwy, aktywne wykrywanie jest wykrywalne, ale nie można wykryć pasywnego sniffowania W sieciach używających koncentratorów lub mediów bezprzewodowych do łączenia systemów, wszystkie hosty w sieci mogą widzieć cały ruch; w związku z tym pasywny sniffer pakietów może przechwytywać ruch do wszystkich hostów połączonych za pośrednictwem koncentratora. Sieć komutowana działa inaczej. Przełącznik sprawdza przesłane dane i próbuje przekazać pakiety do ich zamierzonych odbiorców na

podstawie adresu MAC. Przełącznik utrzymuje tabelę MAC wszystkich systemów i numerów portów, z którymi są połączone. Dzięki temu przełącznik może segmentować ruch sieciowy i wysyłać ruch tylko do prawidłowych docelowych adresów MAC. Sieć przełączników znacznie poprawiła przepustowość i jest bezpieczniejsza niż sieć współdzielona za pośrednictwem koncentratorów. Innym sposobem na wykrywanie danych za pomocą przełącznika jest użycie zakresu portu lub dublowania portów, aby umożliwić duplikowanie wszystkich danych wysyłanych do fizycznego portu przełącznika do innego portu. W wielu przypadkach pule zakresów są używane przez administratorów sieci do monitorowania ruchu w uzasadnionych celach.

Sniffowanie. Środki zaradcze

Najlepszym zabezpieczeniem przed snifferem w sieci jest szyfrowanie. Chociaż szyfrowanie nie przeszkodzi w podsłuchiwaniu, powoduje, że wszelkie dane przechwycone podczas ataku węszącego są bezużyteczne, ponieważ hakerzy nie mogą interpretować tych informacji. Szyfrowanie takie jak AES i RC4 lub RC5 może być wykorzystywane w technologiach VPN i jest powszechnie stosowane w celu zapobiegania podsłuchom w sieci.

Narzędzia przeciwdziałania

NetIntercept to zapora ogniowa i wirusowa. Posiada zaawansowane opcje filtrowania i może się uczyć i dostosowywać, ponieważ identyfikuje nowy spam. Przechwytuje również i kwarantannie najnowsze wirusy i trojany poczty e-mail, zapobiegając instalowaniu trojana i instalowaniu sniffera.

Sniffdet to zestaw testów do zdalnego wykrywania snifferów w środowiskach sieciowych TCP / IP. Sniffdet wdraża różne testy do wykrywania maszyn działających w trybie osiedlania lub za pomocą sniffera.

WinTCPKill to narzędzie do kończenia połączeń TCP dla systemu Windows. Narzędzie wymaga możliwości użycia sniffera do sniffowania ruchu przychodzącego i wychodzącego celu. W sieci komutowanej,

WinTCPKill może używać narzędzia zatrucia pamięci podręcznej ARP, które wykonuje fałszowanie ARP.

Pomijanie ograniczeń przełączników

Ze względu na sposób działania przełączników Ethernet, trudniej jest zbierać przydatne informacje podczas podsłuchu w sieci komutowanej. Ponieważ większość nowoczesnych sieci została zaktualizowana z koncentratora na przełączniki, potrzeba trochę więcej wysiłku, by sniffować sieć komutowaną. Jednym ze sposobów, aby to zrobić, jest oszukanie przełącznika przez wysyłanie danych do komputera hakerów za pomocą zatrucia ARP.

Jak działa ARP

ARP pozwala sieci tłumaczyć adresy IP na adresy MAC. Gdy jeden host korzystający z protokołu TCP / IP w sieci LAN próbuje nawiązać połączenie z innym, potrzebuje adresu MAC lub adresu sprzętowego hosta, do którego próbuje dotrzeć. Najpierw przegląda swoją pamięć podręczną ARP, aby sprawdzić, czy ma już adres MAC; jeśli nie, wysyła żądanie ARP z pytaniem "Kto ma adres IP, którego szukam?" Jeśli host, który ma ten adres IP, słyszy zapytanie ARP, odpowiada swoim własnym adresem MAC i konwersacją może rozpocząć korzystanie z protokołu TCP / IP. Zatrucie ARP to technika używana do atakowania sieci Ethernet, która może pozwolić osobie atakującej na wykrycie ramek danych w przełączanej sieci LAN lub całkowite zatrzymanie ruchu. Zatrucie ARP wykorzystuje fałszowanie ARP, w którym celem jest wysyłanie fałszywych lub sfałszowanych komunikatów ARP do sieci Ethernet LAN. Ramki te zawierają fałszywe adresy MAC, które mylą urządzenia sieciowe, takie jak przełączniki

sieciowe. W rezultacie ramki przeznaczone dla jednego komputera mogą zostać omyłkowo wysłane do innego (umożliwiającego podsłuchiwanie pakietów) lub do nieosiągalnego hosta (odmowa usługi lub DoS, atak). Podszywanie ARP może być również użyte w ataku typu "man-in-the-middle", w którym cały ruch jest przekazywany przez hosta za pomocą spoofingu ARP i analizowany pod kątem haseł i innych informacji.

Środki przeciwdziałające fałszowaniu i zatruwaniu ARP

Aby zapobiec fałszowaniu ARP, trwale dodaj adres MAC bramy do pamięci podręcznej ARP w systemie. Możesz to zrobić w systemie Windows, używając polecenia ARP -s w linii poleceń i dołączając adresy IP bramy i MAC. Takie postępowanie uniemożliwia hakerowi nadpisanie pamięci podręcznej ARP w celu wykonania spoofingu ARP w systemie, ale może być trudne do zarządzania w dużym środowisku z powodu dużej liczby systemów. W środowisku korporacyjnym zabezpieczenia na portach można włączyć w przełączniku, aby umożliwić tylko jeden adres MAC na port przełącznika. W ćwiczeniu 6.1 użyjesz Wiresharka do sniffowania ruchu.

Ćwiczenie 6.1

Użyj Wireshark, aby sniffować ruch

1. Pobierz i zainstaluj najnowszą stabilną wersję Wireshark z www.wireshark.org.

2. Kliknij menu Capture, a następnie wybierz interfejsy.

3. Kliknij przycisk Start obok interfejsu, który pokazuje wysyłane i odbierane pakiety. Jeśli masz wiele interfejsów z aktywnością pakietów, wybierz jedną z nich - najlepiej interfejs o największej aktywności.

4. Kliknij pakiet, aby przeanalizować ten pojedynczy pakiet. Szczegółowe nagłówki będą wyświetlane poniżej ekranu przechwytywania pakietów.

5. Rozwiń każdy nagłówek (IP, TCP) pakietu i określ informacje o adresie.

To ćwiczenie zapewni znacznie większy ruch w sieci, jeśli zostanie wykonane na koncentratorze, a nie na przełączniku. Można użyć sieci bezprzewodowej, ponieważ bezprzewodowa sieć LAN jest dzielonym segmentem sieci podobnym do działania huba.

Narzędzia hakerskie

Wireshark to darmowy sniffer, który może przechwytywać pakiety z przewodowej lub połączenie bezprzewodowej sieci LAN. Oprogramowanie było wcześniej nazywane Ethereal. Wireshark jest powszechnym i popularnym programem, ponieważ jest bezpłatny, ale ma pewne wady. Nieprzeszkolony użytkownik może mieć trudności w pisaniu filtrów w Wireshark, aby przechwytywać tylko niektóre rodzaje ruchu.

Snort to system wykrywania włamań (IDS), który ma również funkcje sniffer. Może być używany do wykrywania różnych ataków i sond, takich jak przepełnienie bufora, port stealth skany, ataki Common Gateway Interface (CGI), sondy SMB (Server Message Block), i próby pobrania odcisków palców w systemie operacyjnym.

WinDump jest wersją systemu Windows tcpdump, analizatora sieci wiersza poleceń dla Unix. WinDump jest w pełni kompatybilny z tcpdump i może być używany do oglądania, diagnozowania, i zapisywanie w ruchu sieciowym dysku zgodnie z różnymi regułami.

EtherPeek to świetny sniffer dla sieci przewodowych z rozbudowanym filtrowaniem i konwersacją TCP / IP możliwości śledzenia. Najnowsza wersja EtherPeek została przemianowana na OmniPeek.

WinSniffer to skuteczny sniffer z hasłem. Monitoruje sieć przychodzącą i wychodzącą ruchu i dekoduje FTP, POP3, HTTP, ICQ, protokół SMTP (Simple Mail Transfer Protocol), telnet, protokół IMAP (Internet Message Access Protocol) oraz nazwy i hasła NNTP (Network News Transfer Protocol).

Iris to zaawansowany analizator danych i ruchu sieciowego, który zbiera, przechowuje, organizuje i raportuje cały ruch danych w sieci. W przeciwieństwie do innych snifferów sieci, Iris jest w stanie zrekonstruować ruch sieciowy, taki jak grafika, dokumenty i e-maile, w tym załączniki.

Filtry Wireshark

Wireshark to darmowy sniffer, który może przechwytywać pakiety z przewodowego lub bezprzewodowego połączenia LAN. Jest to bardzo potężne narzędzie, które może dostarczyć dane protokołu sieci i warstwy wyższej przechwycone w sieci. Podobnie jak wiele innych programów sieciowych, Wireshark wykorzystuje bibliotekę sieciową pcap do przechwytywania pakietów. Wireshark nazywała się Ethereal do 2006 roku, kiedy główny programista postanowił zmienić nazwę ze względu na prawa autorskie z nazwą Ethereal, która została zarejestrowana przez firmę, którą zdecydował się opuścić w 2006 roku. W ćwiczeniu 6.1 zainstalowałeś i zacząłeś przechwytywać pakiety używając Wireshark. Aby zawęzić ilość informacji zebranych przez Wireshark, możesz użyć filtrów. Filtry te ograniczają ilość przechwytywanych lub wyświetlanych informacji.

Oto kilka przykładów filtrów Wireshark:

ip.dst eq www.eccouncil.org Ustawia filtr do przechwytywania tylko pakietów przeznaczonych dla serwera internetowego www.eccouncil.org.

ip.src == 192.168.1.1 Ustawia filtr przechwytujący tylko pakiety przychodzące z hosta

192.168.1.1.

eth.dst eq ff: ff: ff: ff: ff: ff Ustawia filtr do przechwytywania tylko pakietów emisji w warstwie 2.

host 172.18.5.4 Ustawia filtr do przechwytywania tylko ruchu do lub z adresu IP 172.18.5.4.

net 192.168.0.0/24 Ustawia to filtr do przechwytywania ruchu do lub z zakresu adresów IP

port 80 Ustawia filtr do przechwytywania ruchu do portu docelowego 80 (HTTP).

port 80 i tcp [((tcp [12: 1] i 0xf0) >> 2): 4] = 0x47455420 Ustawia filtr na przechwytuje żądania HTTP GET. Filtr szuka bajtów "G", "E", "T" i " " (wartości szesnastkowe 47, 45, 54 i 20) tuż po nagłówku TCP. "Tcp [12: 1] i 0xf0) >> 2" wylicza wartość długości nagłówka TCP.

W ćwiczeniu 6.2 pokazano, jak pisać filtry w Wireshark.

Ćwiczenie 6. 2

Utwórz filtr Wiresharka, aby przechwytywać tylko ruch do lub z adresu IP

1. Otwórz Wireshark.

2. Kliknij aktywny interfejs sieciowy, aby przechwycić ruch.

3. Kliknij Capture, a następnie wybierz filtry.

4. Kliknij nowy przycisk, aby utworzyć nowy filtr.

5. Nazwij nowy filtr w polu nazwy filtra.

6. Wpisz adres IP hosta w polu filtru.

7. Kliknij OK.

8. Wybierz menu przechwytywania i kliknij przycisk start, aby rozpocząć przechwytywanie.

Powtórz powyższe kroki, aby utworzyć filtry, używając następujących ciągów:

net 192.168.0.0/24 Aby przechwytywać ruch do lub z zakresu adresów IP.

src net 192.168.0.0/24 Do przechwytywania ruchu z zakresu adresów IP.

dst net 192.168.0.0/24 Do przechwytywania ruchu do zakresu adresów IP.

port 53 Aby przechwycić tylko ruch DNS (port 53).

host www.example.com i nie (port 80 lub port 25) Aby przechwycić nie-HTTP i nie-ruch SMTP na twoim serwerze.

port nie 53, a nie arp Do przechwytywania wszystkich z wyjątkiem ruchu ARP i DNS.

tcp portrange 1501-1549 Do przechwytywania ruchu w zakresie portów.

nie rozgłaszaj, i nie multicast Przechwytuj tylko ruch emisji pojedynczej. Przydatne, aby pozbyć się szumu w sieci, jeśli chcesz wyświetlać ruch do iz komputera.

Ćwicz zapisywanie filtrów w Wireshark, które przechwytują tylko jeden typ ruchu protokołowego lub ruch z określonego źródła adresu IP lub MAC. Użyj adresu IP lub MAC komputera, aby sprawdzić, czy filtr działa. Ważne jest, aby zrozumieć, jak utworzyć te filtry.

Zrozumienie floding MAC i fałszowania DNS

Sniffer pakietów w sieci komutowanej nie może przechwytywać całego ruchu sieciowego w sieci koncentratora; zamiast tego rejestruje ruch pochodzący z systemu lub przechodzący do niego. Konieczne jest użycie dodatkowego narzędzia do przechwytywania całego ruchu w sieci komutowanej. Zasadniczo istnieją dwa sposoby wykonywania aktywnego podsłuchiwania i sprawiają, że przełącznik wysyła ruch do systemu z uruchomionym snifferem:

ARP Spoofing : Ta metoda polega na użyciu adresu MAC bramy sieciowej i konsekwentnego odbierania całego ruchu przeznaczonego dla bramy w systemie sniffer. Haker może również zalać przełącznik o tak dużym natężeniu ruchu, że przestaje działać jako przełącznik, a zamiast tego powraca do działania jako hub, wysyłając cały ruch do wszystkich portów. Ten aktywny atak sniffujący pozwala systemowi ze snifferem na przechwycenie całego ruchu w sieci.

Wiele przełączników zostało załatanych lub przeprojektowanych tak, aby nie były podatne na podatność na powódź.

DNS Spoofing (lub zatruwanie DNS): Jest to technika, która nakłania serwer DNS do przekonania, że otrzymał autentyczne informacje, podczas gdy w rzeczywistości tak się nie stało. Po zatruciu serwera DNS informacje są generalnie buforowane przez pewien czas, rozprzestrzeniając efekt ataku na użytkowników serwera. Gdy użytkownik zażąda określonego adresu URL witryny, adres zostanie wyświetlony na serwerze DNS, aby znaleźć odpowiedni adres IP. Jeśli serwer DNS został naruszony, użytkownik jest przekierowywany do witryny innej niż ta, której zażądano, takiej jak fałszywa strona internetowa.

Aby wykonać atak DNS, atakujący wykorzystuje lukę w oprogramowaniu serwera DNS, która może spowodować, że zaakceptuje niepoprawne informacje. Jeśli serwer nie sprawdza poprawnie odpowiedzi DNS, aby upewnić się, że pochodzą one z autoryzownego źródła, serwer kończy buforowanie niepoprawnych wpisów lokalnie i udostępnianie ich użytkownikom, którzy wysyłają kolejne żądania. Technika ta może być wykorzystana do zastąpienia dowolnej treści dla zbioru ofiar treścią wybraną przez atakującego. Na przykład osoba atakująca zatruwa wpisy DNS adresu IP witryny docelowej na danym serwerze DNS, zastępując je adresem IP serwera, który kontroluje haker. Następnie haker tworzy fałszywe wpisy dla plików na tym serwerze o nazwach pasujących do nazw na serwerze docelowym. Pliki te mogą zawierać złośliwą zawartość, na przykład robaka lub wirusa. Użytkownik, którego komputer odwołał się do zatrutego serwera DNS, został oszukany, że treść pochodzi z serwera docelowego i nieświadomie pobiera złośliwą zawartość.

Rodzaje technik spoofingu DNS są następujące:

Intranet Spoofing Działając jako urządzenie w tej samej sieci wewnętrznej

InternetSpoofing : Działając jako urządzenie w Internecie

Zatruwanie DNS serwera proxyL Modyfikowanie wpisów DNS na serwerze proxy, aby użytkownik został przekierowany do innego systemu hosta

Zatruwanie pamięci podręcznej DNS : Modyfikowanie wpisów DNS w dowolnym systemie, aby użytkownik został przekierowany do innego hosta

Narzędzia hakerskie

EtherFlood jest wykorzystywany do zalania przełącznika Ethernet ruchem, aby przywrócić go do trybu koncentratora. W ten sposób haker jest w stanie przechwycić cały ruch w sieci, a nie tylko ruch do i z jego systemu, jak w przypadku przełącznika.

Dsniff to zbiór uniksowych narzędzi do wykonywania audytów sieciowych oraz penetracji sieci. Następujące narzędzia są zawarte w dsniff: filesnarf, mailsnarf, msgsnarf, urlsnarf i webspy. Te narzędzia pasywnie monitorują podatne udostępniane sieci (na przykład sieć LAN, w której sniffer znajduje się za zewnętrzną zaporą sieciową), aby uzyskać interesujące dane (hasła, pocztę e-mail, pliki itd.).

Sshmitm i webmitm realizują aktywne ataki typu "man-in-the-middle" przeciwko przekierowanym sesjom Secure Shell (SSH) i HTTPS.

Arpspoof, dnsspoof i macof działają na przechwytywanie przełączanego ruchu sieciowego, który jest zwykle niedostępny dla programu sniffer z powodu przełączania. Aby poradzić sobie z problemem przełączania pakietów warstwy 2, dsniff podszywa się pod sieć, myślącą, że jest bramą, przez którą dane muszą przejść, aby wyjść poza sieć.

IP Restrictions Scanner (IRS) służy do wyszukiwania ograniczeń IP, które zostały ustawione dla określonej usługi na hoście. Łączy w sobie zatrucie ARP z techniką ukrywania lub połowicznego skanowania TCP i wyczerpująco testuje wszystkie możliwe fałszywe połączenia TCP z wybranym portem docelowym. IRS może znajdować serwery i urządzenia sieciowe, takie jak routery i przełączniki, oraz identyfikować funkcje kontroli dostępu, takie jak listy kontroli dostępu (ACL), filtry IP i reguły zapory ogniowej.

sTerm jest klientem Telnet z unikalną funkcją: może ustanowić dwukierunkową sesję telnetu do hosta docelowego, bez wysyłania prawdziwych adresów IP i MAC w żadnym pakiecie. Wykorzystując zatrucie

ARP, podszywanie się pod MAC i podszywanie się pod IP, sTerm może skutecznie ominąć listy ACL, reguły firewalla i ograniczenia IP na serwerach i urządzeniach sieciowych.

Cain & Abel to uniwersalne narzędzie hakerskie dla systemu Windows. Pozwala na łatwe odzyskiwanie różnego rodzaju haseł poprzez węszenie sieci; łamanie zaszyfrowanych haseł przy użyciu słownika lub brutalnych ataków; nagrywanie głosu przez IP lub VoIP, rozmowy; dekodowanie zaszyfrowanych haseł; ujawniające skrzynki z hasłami; odczytywanie haseł w pamięci podręcznej; i analizowanie protokołów routingu. Najnowsza wersja zawiera wiele nowych funkcji, takich jak ARP

Trujący Routing (APR), który umożliwia podsłuchiwanie przełączanych sieci LAN i ataków man-in-the-middle. Sniffer w tej wersji może również analizować zaszyfrowane protokoły, takie jak SSH-1 i HTTPS, i zawiera filtry do przechwytywania poświadczeń z szerokiej gamy mechanizmów uwierzytelniania.

Packet Crafter to narzędzie używane do tworzenia niestandardowych pakietów TCP / IP / UDP. Narzędzie może zmienić adres źródłowy pakietu, który wykonuje podszywanie się pod IP i może kontrolować flagi IP (takie jak sumy kontrolne) i flagi TCP (takie jak flagi stanu, numery sekwencji i numery potwierdzenia).

SMAC to narzędzie używane do zmiany adresu MAC systemu. Pozwala hakerowi podszywać się pod adres MAC podczas wykonywania ataku.

MAC Changer to narzędzie służące do podszywania się pod adres MAC w systemie Unix. Można go użyć do ustawienia interfejsu sieciowego na określony adres MAC, ustawienia MAC losowo, ustawienia adresu MAC innego dostawcy, ustawienia innego adresu MAC tego samego dostawcy, ustawienia adresu MAC tego samego typu lub wyświetlenia listy adresów MAC dostawcy wybrać z.

WinDNSSpoof to proste narzędzie do fałszowania identyfikatorów DNS dla systemu Windows. Aby używać go w sieci komutowanej, musisz być w stanie sniffować ruch atakowanego komputera. W związku z tym może być konieczne użycie go w połączeniu z narzędziem do spoofingu lub zalewania ARP.

Rozproszony DNS Flooder wysyła dużą liczbę zapytań, aby utworzyć atak DoS, wyłączając DNS. Jeśli oprogramowanie demona DNS zarejestruje nieprawidłowe zapytania, wpływ tego ataku zostanie wzmocniony.

Podsumowanie

Sniffing jest nieocenionym narzędziem w zestawie narzędzi etycznego hackera. Sniffing można wykorzystać do zbierania informacji pasywnie i przechwytywania cennych danych, takich jak hasła. Zaletą podsłuchiwania jest to, że można go wykonać pasywnie i jest praktycznie niewykrywalny, gdy jest używany w trybie pasywnym. Bardziej agresywne metody wąchania, takie jak zatrucie ARP i podszywanie się pod DNS, mogą być stosowane, jeśli bierne węszenie nie przyniesie informacji, które CEH chce zebrać. Wystarczy uprzedzić, że te aktywne metody mogą zostać wykryte i ostrzec pracowników ochrony przed atakiem w sieci.

Do Zapamiętania!

* Dowiedziałeś się, jak działa sniffer. Sniffer działa w trybie mieszanym, co oznacza, że przechwytuje cały ruch, niezależnie od docelowego adresu MAC określonego w ramce.

* Zapoznałeś się z różnicami między podsłuchiwaniem w sieci współdzielonej przez huby i przełączaną sieć. Cały ruch jest transmitowany przez koncentrator, ale jest podzielony na segmenty za pomocą

przełącznika. Aby powąchać włączoną sieć, należy użyć narzędzi do podszywania się lub podszywania się pod ARP.

* Poznałeś różnicę między pakietami i ramkami. Pakiety są tworzone na Warstwie 3 modelu OSI, a ramki są tworzone na Warstwie 2.

* Dowiedziałeś się, jak działa protokół ARP (Address Resolution Protocol). ARP służy do znalezienia adresu MAC ze znanego adresu IP przez rozgłaszanie żądania w sieci.

* Poznałeś różnicę pomiędzy aktywnym i pasywnym wąchaniem. Aktywne węszenie służy do okiełznania przełącznika do działania w stylu koncentratora, tak aby przekazywał ruch do atakującego. Pasywne podsłuchiwanie przechwytuje pakiety, które są już transmitowane w sieci wspólnej.