Skanowanie jest pierwszą fazą aktywnego hakowania i służy do lokalizowania docelowych systemów lub sieci w celu późniejszego ataku. Enumeracja jest kolejnym krokiem po zakończeniu skanowania i służy do identyfikowania nazw komputerów, nazw użytkowników i udziałów. Skanowanie i wyliczanie są omówione razem w tym rozdziale, ponieważ wiele narzędzi hakerskich wykonuje jednocześnie oba kroki.

Skanowanie

Po zakończeniu etapów rozpoznania i zbierania informacji przeprowadzane jest skanowanie. Ważne jest, aby etap zbierania informacji był tak kompletny, jak to możliwe, w celu określenia najlepszej lokalizacji i celów do skanowania. Podczas skanowania haker zbiera informacje dotyczące sieci i poszczególnych systemów hosta. Informacje takie jak adresy IP, system operacyjny, usługi i zainstalowane aplikacje mogą pomóc hakerowi w określeniu, jakiego typu exploit może zostać użyty podczas włamań do systemu. Skanowanie jest procesem lokalizowania systemów, które są żywe i reagują w sieci. Etyczni hakerzy używają skanowania w celu identyfikacji adresów IP systemów docelowych. Skanowanie służy również do określenia, czy system jest w sieci i czy jest dostępny. Narzędzia skanujące służą do gromadzenia informacji o systemie, takich jak adresy IP, system operacyjny i usługi uruchomione na komputerze docelowym. Tabela zawiera listę trzech typów skanowania.

Typ skanowania :	Cel
Skanowanie portów :	Określa otwarte porty i usługi
Skanowanie sieciowe :	Identyfikuje adresy IP w danej sieci lub podsieci
Skanowanie podatności :	Odkrywa obecność znanych słabości w systemach docelowych

Skanowanie portów Skanowanie portów to proces identyfikowania otwartych i dostępnych portów TCP / IP w systemie.

Narzędzia do skanowania portów umożliwiają hakerom poznanie dostępnych usługa firmy jest kluczem do zapobiegania atakom socjotechnicznym. Narzędzia do skanowania portów umożliwiają hakerom poznanie usług dostępnych w danym systemie. Każda usługa lub aplikacja na komputerze jest powiązana z dobrze znanym numerem portu. Numery portów są podzielone na trzy zakresy:

* Dobrze znane porty: 0-1023

* Zarejestrowane Porty: 1024-49151

* Dynamiczne Porty: 49152-65535

Na przykład narzędzie do skanowania portów, które identyfikuje port 80 jako otwarty, wskazuje, że serwer internetowy działa w tym systemie. Hakerzy muszą znać dobrze znane numery portów

Wspólne numery portów

W systemach Windows dobrze znane numery portów znajdują się w pliku C: \ windows \ system32 \drivers \ etc \ services. sercices to ukryty plik. Aby go wyświetlić, pokaż ukryte pliki w systemie Windows Explorer i kliknij dwukrotnie nazwę pliku, aby otworzyć go za pomocą Notatnika. Zapoznaj się z numerami portów dla następujących aplikacji:

* FTP, 21

* Telnet, 23

* HTTP, 80

* SMTP, 25

* POP3, 110

* HTTPS, 443

Poniższa lista zawiera dodatkowe numery portów przydatnych do testowania penetracyjnego w świecie rzeczywistym:

* Global Catalog Server (TCP), 3269 i 3268

* Serwer NN LDAP (TCP / UDP), 389

* LDAP SSL (TCP / UDP), 636

* IPsec ISAKMP (UDP), 500

* NAT-T (UDP), 4500

* RPC (TCP), 135

* Stan sesji ASP.NET (TCP), 42424

* Usługa NetBIOS Datagram Service (UDP), 137 i 138

* Usługa NetBIOS Session Service (TCP), 139

* Serwer DHCP (UDP), 67

* Serwer LDAP (TCP / UDP), 389

* SMB (TCP), 445

* RPC (TCP), 135

* DNS (TCP / UDP), 53

* IMAP (TCP), 143

* IMAP przez SSL (TCP), 993

* POP3 (TCP), 110

* POP3 przez SSL (TCP), 995

* RPC (TCP), 135

* RPC przez HTTPS (TCP), 443 lub 80

* SMTP (TCP / UDP), 25

Skanowanie sieciowe Skanowanie sieciowe jest procedurą służącą do identyfikowania aktywnych hostów w sieci w celu ich zaatakowania lub oceny bezpieczeństwa sieci. Hosty są identyfikowane przez ich indywidualne adresy IP. Narzędzia do skanowania sieci próbują zidentyfikować wszystkie hosty na żywo lub odpowiadające w sieci i odpowiadające im adresy IP.

Skanowanie luk Skanowanie słabości to proces proaktywnej identyfikacji luk w zabezpieczeniach systemów komputerowych w sieci. Ogólnie skaner słabości narażenia na atak najpierw identyfikuje system operacyjny i numer wersji, w tym dodatki Service Pack, które mogą być zainstalowane. Następnie skaner identyfikuje słabe punkty lub luki w systemie operacyjnym. Podczas późniejszej fazy ataku haker może wykorzystać te słabości, aby uzyskać dostęp do systemu.

Chociaż skanowanie może szybko zidentyfikować, które hosty nasłuchują i są aktywne w sieci, jest to również szybki sposób identyfikacji za pomocą systemu wykrywania włamań (IDS). Narzędzia skanujące badają porty TCP / IP, szukając otwartych portów i adresów IP, a te sondy są rozpoznawane przez większość narzędzi do wykrywania włamań. Skanowanie sieci i wykrywanie luk może być zwykle wykrywane, ponieważ skaner musi wchodzić w interakcję z systemem docelowym przez sieć. W zależności od typu aplikacji skanującej i szybkości skanowania, IDS wykryje skanowanie i zgłosi je jako zdarzenie IDS. Niektóre narzędzia do skanowania mają różne tryby próbujące pokonać IDS i są bardziej prawdopodobne, że będą w stanie skanować niewykryte.

Metodologia skanowania

Jako od etycznego hackera, oczekuje się, że zapoznasz się z metodologią skanowania przedstawioną poniżej:

Sprawdź działające systemy

Sprawdź otwarte porty

Identyfikacja usługi

Pobieranie transparentów / Odciski palców OS

Skanowanie luk

Narysuj schematy sieciowe hostów narażonych na ataki

Przygotuj serwery proxy

Atak

Ta metodologia jest procesem, w którym haker skanuje sieć. Gwarantuje to, że nie zostanie przeoczony żaden system lub luka w zabezpieczeniach i że haker zbierze wszystkie informacje niezbędne do przeprowadzenia ataku. Przyjrzymy się poszczególnym etapom tej metodologii skanowania poczynając od pierwszych trzech kroków - sprawdzenia systemów działających i otwartych portów oraz identyfikacji usług - w poniższej sekcji.

Techniki Ping Sweep

Metodyka skanowania rozpoczyna się od sprawdzenia systemów działających w sieci, co oznacza, że odpowiadają one na zapytania lub żądania połączeń. Najprostszym, choć niekoniecznie najdokładniejszym sposobem ustalenia, czy systemy są aktywne, jest wykonanie polecenia "ping sweep" zakresu adresów IP. Wszystkie systemy, które odpowiadają za pomocą polecenia ping, są traktowane jako żywe w sieci. Przeszukiwanie w trybie ping jest również znane jako skanowanie protokołu ICMP (Internet Control Message Protocol), ponieważ protokół ICMP jest używany przez polecenie ping. Skanowanie ICMP lub pingowanie to proces wysyłania żądania ICMP lub polecenia ping do wszystkich hostów w sieci w celu określenia, które z nich są uruchomione i reagują na pingi. Protokół ICMP został uruchomiony jako protokół używany do wysyłania komunikatów testowych i komunikatów o błędach między hostami w Internecie. Rozwinął się jako protokół wykorzystywany przez każdy

system operacyjny, router, przełącznik lub protokół internetowy (IP). Możliwość korzystania z żądania echa ICMP i odpowiedzi echa jako testu łączności między hostami jest wbudowana w każde urządzenie z obsługą IP za pomocą polecenia ping. Jest to szybki i brudny test, aby sprawdzić, czy dwa hosty mają łączność i są szeroko wykorzystywane do rozwiązywania problemów. Zaletą skanowania ICMP jest to, że może być uruchamiany równolegle, co oznacza, że wszystkie systemy są skanowane w tym samym czasie; dzięki temu może działać szybko w całej sieci. Większość narzędzi hakerskich obejmuje opcję ping-sweep, co w praktyce oznacza wykonanie żądania ICMP dla każdego hosta w sieci. Systemy, które reagują odpowiedzią ping, są żywe i nasłuchują w sieci. W ćwiczeniu 3.1 pokazano, jak wykonać sweep za pomocą wbudowanych narzędzi systemu Windows. Istotnym problemem związanym z tą metodą jest to, że osobiste zapory sieciowe i sieciowe zapory ogniowe mogą blokować system przed reagowaniem na pingowanie. Coraz więcej systemów jest konfigurowanych za pomocą zapory sieciowej i blokuje próbę pingowania oraz powiadamia użytkownika, że program do skanowania działa w sieci. Innym problemem jest to, że komputer musi być włączony, aby zostać zeskanowany.

Wskazania ataku skanującego

Bob pracuje na swoim laptopie podczas w podróży służbowej poza biurem. Korzysta z bezpłatnego bezprzewodowego dostępu do Internetu w swoim komputerze. Wysyłając wiadomość e-mail, widzi wyskakujące okno na pasku zadań swojego komputera z systemem Windows XP. Mówi "Windows wykrył i zablokował próbę włamania do twojego komputera." Zamyka tylko wyskakujące okienko i wraca, aby zakończyć pisanie e-maila. Następnie zauważa kolejne wyskakujące okienko z podobnym przekazem. Zaczyna martwić się, że jego komputer jest zhackowany. Decyduje się zamknąć laptopa, aby żadne inne próby połączenia z jego komputerem nie były możliwe.

Narzędzia hakerskie

Pinger, Friendly Pinger i WS_Ping_Pro to wszystkie narzędzia, które wykonują kwerendy ICMP.

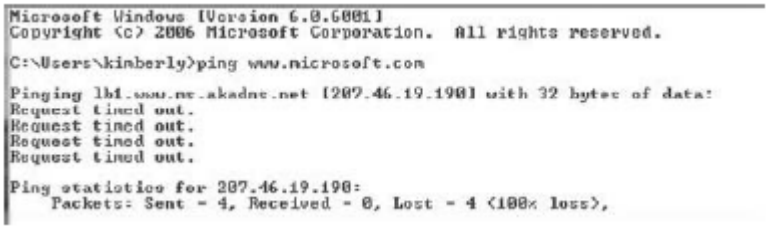
Ćwiczenie 3.1

Korzystanie z Ping Windows

Aby użyć wbudowanego polecenia ping w systemie Windows, aby przetestować łączność z innym systemem:

1. Otwórz wiersz polecenia w systemie Windows.

2. Wpisz polecenie ping www.microsoft.com.



Timeout wskazuje, że system zdalny nie odpowiada lub jest wyłączony lub że ping został zablokowany. Odpowiedź wskazuje, że system jest żywy i odpowiada na żądania ICMP.

Wykrywanie Ping Sweep

Prawie każdy system IDS lub systemu zapobiegania włamaniom (IPS) wykryje i powiadomi administratora zabezpieczeń o wykreśleniu pingów w sieci. Większość zapór ogniowych i serwerów

proxy blokuje odpowiedzi ping, więc haker nie może dokładnie określić, czy systemy są dostępne za pomocą samego trybu ping. Jeśli systemy nie reagują na zamiatanie przez ping, należy użyć bardziej intensywnego skanowania portów. Tylko dlatego, że ping sweep nie zwraca żadnych aktywnych hostów w sieci, nie oznacza, że nie są one dostępne - musisz spróbować alternatywnej metody identyfikacji. Pamiętaj, że hakowanie wymaga czasu, cierpliwości i wytrwałości.

Skanowanie portów i identyfikowanie usług

Sprawdzanie otwartych portów jest drugim krokiem w metodologii skanowania. Skanowanie portów to metoda używana do sprawdzania otwartych portów. Proces skanowania portów obejmuje sondowanie każdego portu na hoście w celu określenia, które porty są otwarte. Skanowanie portów ogólnie dostarcza więcej cennych informacji niż zamiatanie pingami na temat hosta i luk w systemie. Identyfikacja usług jest trzecim krokiem w metodologii skanowania; zwykle odbywa się za pomocą tych samych narzędzi, co skanowanie portów. Identyfikując otwarte porty, haker może zazwyczaj zidentyfikować usługi związane z tym numerem portu.

Środki zaradcze przed skanowaniem portów

Środki zaradcze to procesy lub zestawy narzędzi wykorzystywane przez administratorów zabezpieczeń do wykrywania i prawdopodobnie udaremniania skanowania portów hostów w ich sieci. Poniższa lista środków zaradczych powinna zostać zaimplementowana, aby zapobiec przejęciu przez hakera informacji podczas skanowania portu:

* Należy przestrzegać odpowiedniej architektury zabezpieczeń, takiej jak implementacja I NN DS i zapór ogniowych.

* Etyczni hakerzy używają swojego zestawu narzędzi do testowania środków zaradczych związanych ze skanowaniem, które zostały zaimplementowane. Po zainstalowaniu zapory należy uruchomić narzędzie do skanowania portów względem hostów w sieci, aby ustalić, czy zapora prawidłowo wykrywa i zatrzymuje działanie skanowania portów.

* Zapora sieciowa powinna być w stanie wykryć sondy wysyłane przez narzędzia do skanowania portów. Zapora sieciowa powinna przeprowadzać kontrole stanowe, co oznacza, że analizuje dane pakietu, a nie tylko nagłówek TCP, aby określić, czy ruch może przepływać przez zaporę.

* Identyfikator sieci powinien być używany do identyfikacji metody wykrywania systemu operacyjnego używanej przez niektóre typowe narzędzia hakerów.

* Tylko potrzebne porty powinny być otwarte. Reszta powinna być filtrowana lub blokowana.

* Personel organizacji korzystający z systemów powinien przejść odpowiednie szkolenie w sprawie świadomości bezpieczeństwa. Powinni także znać różne zasady bezpieczeństwa, którymi się kierują a są wymagane do naśladowania.

Przełączniki poleceń nmap

nmap to darmowe narzędzie o otwartym kodzie źródłowym, które szybko i wydajnie wykonuje skanowanie w pętli, skanowanie portów, identyfikację usług, wykrywanie adresów IP i wykrywanie systemu operacyjnego. nmap ma zaletę skanowania dużej liczby maszyn w jednej sesji. Jest obsługiwany przez wiele systemów operacyjnych, w tym Unix, Windows i Linux. Stan portu określony przez skanowanie nmap może być otwarty, filtrowany lub niefiltrowany. Otwarty oznacza, że komputer docelowy akceptuje przychodzące żądanie na tym porcie. Filtrowanie oznacza, że firewall lub filtr sieciowy filtruje port i uniemożliwia programowi nmap odkrywanie, czy jest on otwarty. Niefiltrowane

oznacza, że port jest określony jako zamknięty, a żadna zapora ani filtr nie zakłócają żądań nmap. nmap obsługuje kilka typów skanów. Tabela poniższa zawiera szczegóły typowej metody skanowania

Typ skanowania Nmap :	Opis
Połączenie TCP :	Osoba atakująca tworzy pełne połączenie TCP z systemem docelowym. Najbardziej niezawodny typ skanowania, ale także najbardziej wykrywalny. Otwórz odpowiedzi portów z SYN / ACK, gdy zamknięte porty odpowiedzą RST / ACK.
Skanowanie drzewa XMAS :	Atakujący sprawdza usługi TCP wysyłając pakiety drzewa XMAS, które są nazywane jako takie, ponieważ wszystkie "światła" są włączone, co oznacza ,że Flagi FIN, URG i PSH są ustawione . Porty zamknięte odpowiadają flagą RST.
Skanowanie ukrycia SYN :	Jest to tak zwane skanowanie półotwarte. Haker wysyła pakiet SYN i otrzymuje SYN-ACK z serwera. Jest ukradkowy ponieważ pełne połączenie TCP nie jest otwierane. Otwarte porty odpowiedzią za pomocą SYN / ACK w zamkniętych portach odpowiedz z RST / ACK.
Skanowanie zerowe :	To zaawansowane skanowanie, które może przejść przez zapory ogniowe niewykryte lub zmodyfikowane. Skanowanie zerowe ma wyłączone wszystkie flagi lub nie jest ustawione. Tylko działa na systemach uniksowych. Zamknięte porty zwrócą flagę RST.
Skanowanie systemu Windows :	Ten typ skanowania jest podobny do skanowania ACK i może również wykrywać otwarte porty.
Skanowanie ACK :	Ten typ skanowania służy do mapowania reguł zapory sieciowej. Skanowanie ACK działa tylko na Unix. Port jest uważany za filtrowany przez reguły zapory, jeśli jest miejscem docelowym ICMP nieosiągalny komunikat jest otrzymywany w wyniku skanowania ACK.

Polecenie nmap ma wiele przełączników do wykonywania różnych typów skanów. Typowe przełączniki poleceń są wymienione w tabeli:

przełącznik polecenia nmap :	Wykonane skanowanie
-sT	Skanuj połączenie TCP
-sS	Skanowanie SYN
-sF	Skanowanie FIN
-sX	Skanowanie drzewa XMAS
-sN	Skanowanie Null
-sP	Skanowanie ping

-sU	Skanowanie UDP
-sO	Skanowanie protokołu
-sA	Skanowanie ACK
-sW	Skanowanie systemu Windows
-sR	Skanowanie RPC
-sL	Lista / skanowanie DNS
-sI	Skanowanie w trybie bezczynności
-Po	Nie pinguj
-PT	TCP ping
-PS	SYN ping
-PI	ping ICMP
-PB	TCP i ping ICMP
-PB	Znacznik czasu ICMP
-PM	Maska sieci ICMP
-oN	Normalne wyjście
-oX	wyjście XML
-oG	Dane wyjściowe możliwe do wywołania
-oA	Wszystkie dane wyjściowe
-T Paranoid	Skanowanie szeregowe; 300 s między skanami
-T Sneaky	Skanowanie szeregowe; 15 s między skanami
-T Polite	Skanowanie szeregowe; 4 s między skanami
-T Normal	Skanowanie równoległe
-T Agressive	Skanowanie równoległe, limit czasu 300 sekund i 1,25 sekundy / próbę
-T Insame	Skanowanie równoległe, limit czasu 75 sekund i 35 sekundy / próbę

Aby wykonać skanowanie nmap, w wierszu poleceń systemu Windows wpisz Nmap IPaddress, a następnie dowolne przełączniki poleceń używane do wykonywania określonego typu skanów. Na przykład, aby przeskanować host z adresem IP 192.168.0.1 za pomocą typu skanowania połączenia TCP, wprowadź następujące polecenie:

Nmap 192.168.0.1 –sT

Typy skanowania

Jako etyczny hacker musisz znać następujące typy i zastosowania skanowania:

SYN Skanowanie SYN lub stealth jest nazywany skanem półotwartym, ponieważ nie kończy on trójstronnego uzgadniania TCP. (Trzydrożny handshake TCP / IP zostanie omówiony w następnej sekcji.) Haker wysyła pakiet SYN do celu; jeśli odebrana zostanie ramka SYN / ACK, to zakłada się, że cel zakończy połączenie, a port nasłuchuje. Jeśli RST jest odbierany z powrotem od celu, to zakłada się, że port nie jest aktywny lub jest zamknięty. Zaletą stealth SYN jest to, że mniej systemów IDS rejestruje to jako atak lub próbę połączenia.

XMAS Skanowanie XMAS wysyłają pakiet z ustawionymi flagami FIN, URG i PSH. Jeśli port jest otwarty, nie ma odpowiedzi; ale jeśli port jest zamknięty, cel odpowiada pakietem RST / ACK. Skanowanie XMAS działa tylko w systemach docelowych zgodnych z implementacją protokołu TCP / IP RFC 793 i nie działa w stosunku do żadnej wersji systemu Windows.

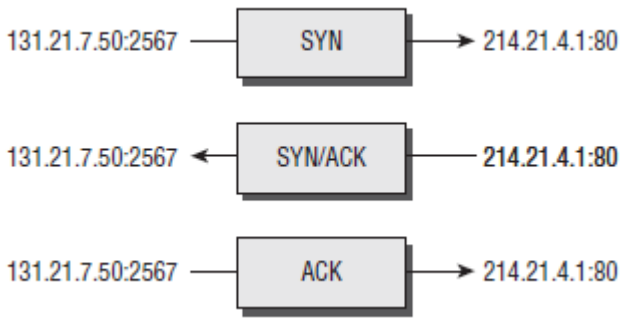
FIN Skanowanie FIN jest podobny do skanowania XMAS, ale wysyła pakiet z ustawionym tylko flagą FIN. Skany FIN otrzymują odpowiedź samemu i mają te same ograniczenia co skanowanie XMAS.

NULL Skanowanie NULL jest również podobne do XMAS i FIN w zakresie jego ograniczeń i reakcji, ale po prostu wysyła pakiet bez ustawionych flag.

IDLE Skanowanie IDLE używa sfałszowanego adresu IP do wysłania pakietu SYN do celu. W zależności od odpowiedzi port można określić jako otwarty lub zamknięty. Skanowanie IDLE określa odpowiedź skanowania portu, monitorując numery sekwencji nagłówków IP.

Typy flag komunikacji TCP

Typy skanowania TCP są zbudowane na potrójnym uzgadnianiu TCP. Połączenia TCP wymagają trójstronnego uzgadniania przed nawiązaniem połączenia i przesłania danych między nadawcą a odbiorcą. Rysunek 3.2 przedstawia szczegóły potrójnego uzgadniania TCP.



Aby ukończyć potrójne uzgadnianie i nawiązać udane połączenie między dwoma hostami, nadawca musi wysłać pakiet TCP z ustawionym bitem synchronizacji (SYN). Następnie system odbierający odpowiada pakietem TCP z ustawionym bitem synchronizacji (SYN) i potwierdzeniem (ACK), aby wskazać, że host jest gotowy do odbioru danych. System źródłowy wysyła ostatni pakiet z ustawionym bitem ACK, aby wskazać, że połączenie zostało zakończone i dane są gotowe do wysłania. Ponieważ TCP jest protokołem zorientowanym na połączenie, proces ustanawiania połączenia (potrójnego uzgadniania), restartowania nieudanego połączenia i zakończenia połączenia jest częścią protokołu. Te powiadomienia protokołu są nazywane flagami. TCP zawiera flagi ACK, RST, SYN, URG, PSH i FIN. Poniższa lista identyfikuje funkcję flag TCP:

SYN Synchronizuj. Inicjuje połączenie między hostami.

ACK Potwierdzenie. Ustalenie połączenia między hostami.

PSH Push. System przesyła buforowane dane.

URG Pilne. Dane w pakietach muszą być szybko przetworzone.

FIN Finish. Koniec z transmisjami.

RST Resetowanie . Resetuje połączenie.

Haker może próbować ominąć wykrywanie za pomocą flag zamiast normalnego połączenia TCP. Typy skanowania TCP w Tabeli poniższej są używane przez niektóre narzędzia do skanowania w celu wywołania odpowiedzi z systemu przez ustawienie jednej lub więcej flag.

Skanowanie XMAS :	Flagi wysłane przez hakera
Skanowanie XMAS	Wszystkie ustawione flagi (ACK, RST, SYN, URG, PSH, FIN)
Skanowanie FIN	FIN
Skanowanie NULL	Brak ustawionych flag
Połączenie TCP/ otwarte skanowanie	SYN, a następnie ACK
Skanowanie SYN / skanowanie półotwarte	SYN, a następnie RST

Narzędzia hakerskie

IPEye to skaner portów TCP, który może skanować SYN, FIN, Null i XMAS. To narzędzie linii poleceń. IPEye bada porty w systemie docelowym i odpowiada z zamkniętym, odrzuconym, upuszczonym lub otwartym. Zamknięty oznacza, że na drugim końcu znajduje się komputer, ale nie nasłuchuje na porcie. Odrzucony oznacza, że zapora sieciowa odrzuca połączenie z portem (wysyłając reset z powrotem). Upuść oznacza, że zapora sieciowa upuszcza wszystko do portu lub na drugim końcu nie ma komputera. Otwarty oznacza, że jakiś rodzaj usług nasłuchuje w porcie. Odpowiedzi te pomagają hakerowi określić, jaki rodzaj systemu odpowiada. IPSecScan to narzędzie do skanowania pojedynczego adresu IP lub zakresu adresów w poszukiwaniu systemów z włączoną obsługą IPSec. NetScan Tools Pro, hping2, KingPingicmpenum i SNMP Scanner są narzędziami do skanowania i mogą być również wykorzystywane do odcisków palców systemu operacyjnego (omówionych później). Icmpenum wykorzystuje nie tylko pakiety ICMP Echo do testowania sieci, ale także ICMP Datownik i pakiety ICMP Information. Ponadto obsługuje podszywanie się i wąchanie pakietów odpowiedzi. Icmpenum doskonale nadaje się do skanowania sieci, gdy zapora blokuje pakiety ICMP Echo, ale nie blokuje znacznika czasu ani pakietów informacyjnych. Narzędzie hping2 jest godne uwagi, ponieważ zawiera wiele innych funkcji oprócz pobierania odcisków palców z systemu operacyjnego, takich jak protokół TCP, protokół User Datagram Protocol (UDP), protokół ICMP i protokołu Raw-IP ping, tryb traceroute oraz możliwość wysyłania plików między źródłem a celem system. Skaner SNMP umożliwia skanowanie zakresu lub listy hostów wykonujących zapytania ping, DNS i Simple Network Management Protocol (SNMP).

W ćwiczeniu 3.2 pokazano, jak korzystać ze skanera AngryIP w celu przeprowadzenia skanowania portu

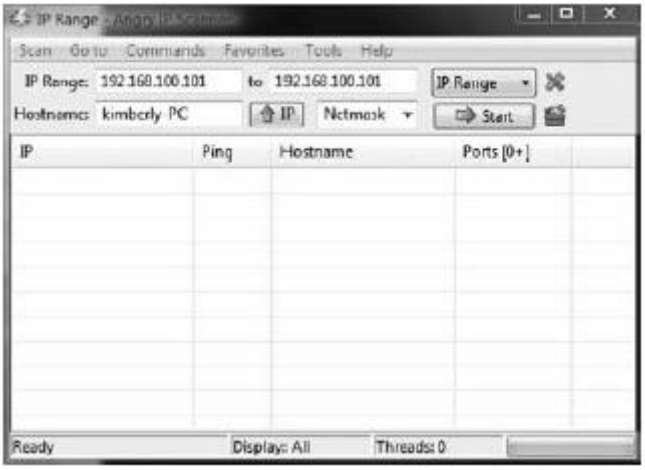
Ćwiczenie 3. 2

Bezpłatne IPTools Port Scan

Aby użyć narzędzia do skanowania portów, aby określić porty nasłuchiwania aktywnych hostów:

1. Pobierz narzędzie Angry IP Scanner ze strony www.angryip.org/w/Download.

2. Wprowadź adres IP systemu docelowego w polu Host lub adres IP lub wprowadź zakres lub adres IP dla systemów laboratoryjnych i kliknij Start, aby wykonać standardowy (pełny łącz) skan standardowych portów.



Techniki War-Dialingu

Wirtualne wybieranie numerów to proces wybierania numerów modemów w celu znalezienia otwartego połączenia modemowego, które zapewnia zdalny dostęp do sieci w celu przeprowadzenia ataku na system docelowy. Termin "wybieranie wojenne" pochodzi z początków istnienia Internetu, kiedy większość firm była podłączona do Internetu za pośrednictwem modemu dial-up. Wybieranie wojenne jest włączone jako metoda skanowania, ponieważ znajduje inne połączenie sieciowe, które może mieć słabsze zabezpieczenia niż główne połączenie internetowe. Wiele organizacji konfiguruje modemy dostępu zdalnego, które są już przestarzałe, ale nie udało się usunąć tych serwerów dostępu zdalnego. To daje hakerom łatwy dostęp do sieci ze znacznie słabszymi mechanizmami bezpieczeństwa. Na przykład wiele systemów zdalnego dostępu korzysta z protokołu uwierzytelniania haseł (PAP), który wysyła hasła w postaci zwykłego tekstu, zamiast nowszej technologii wirtualnej sieci prywatnej (VPN), która szyfruje hasła. Narzędzia do wybierania w czasie działają zgodnie z założeniem, że firmy nie kontrolują portów dial-in tak ściśle, jak firewall, a maszyny z podłączonymi modemami są obecne wszędzie, nawet jeśli te modemy nie są już używane. Wiele serwerów nadal posiada modemy z liniami telefonicznymi podłączonymi jako backup w przypadku awarii podstawowego połączenia z Internetem. Te dostępne połączenia modemowe mogą być używane przez program wybierania w celu uzyskania zdalnego dostępu do systemu i sieci wewnętrznej.

Korzystanie z zapomnianego połączenie modemowe w celu wybrania numeru w war-dialingu

Kilka lat temu przeprowadzałem audyt bezpieczeństwa sieci dla firmy świadczącej usługi finansowe. Poprosili mnie o przejrzenie strony w celu przeprowadzenia audytu bezpieczeństwa fizycznego. Przechodząc obok jednego z biurka w dziale marketingu, zauważyłem linię telefoniczną wychodzącą z biurka i podłączającą się do gniazdka ściennego. Pytałem o użycie modemów, gdy próbowałem ustalić przyczynę kabla linii telefonicznej. Powiedziano mi, że korzystali z połączeń telefonicznych na niektórych komputerach w celu uzyskania dostępu do Internetu, ale dwa lata temu przełączyli się na szybkie połączenie T1 dla całego biura. W miarę dalszego badania okazało się, że pracownik, który korzystał z tego komputera, nadal korzystał z AOL na połączeniu telefonicznym, aby sprawdzić swoje

osobiste konto e-mail. Zaskakujące dla wszystkich, gdy zainstalowano nowe połączenie internetowe, nikt nigdy nie sprawdzał, czy wszystkie połączenia dial-up zostały usunięte. Oto doskonały przykład, dlaczego war dialing nadal działa w niektórych przypadkach.

Narzędzia hakerskie

THC-Scan, PhoneSweep i TeleSweep to narzędzia, które identyfikują numery telefonów i mogą wybierać cel, aby uzyskać połączenie z modemem komputerowym. Narzędzia te działają na ogół za pomocą wcześniej ustalonej listy wspólnych nazw użytkowników i haseł, aby uzyskać dostęp do systemu. Większość połączeń dial-in z dostępem zdalnym nie jest zabezpieczona hasłem ani nie zapewnia bardzo podstawowych zabezpieczeń.

Przechwytywanie bannerów i techniki pobierania odcisków palców

Przechwytywanie banerów i identyfikacja systemu operacyjnego - które można również zdefiniować jako odciski palca stosu TCP / IP - jest czwartym krokiem w metodologii skanowania CEH. Proces pobierania odcisków palców umożliwia hakerowi identyfikację szczególnie zagrożonych lub wartościowych obiektów w sieci. Hakerzy szukają najprostszego sposobu na uzyskanie dostępu do systemu lub sieci. Przechwytywanie banerów to proces otwierania połączenia i odczytywania banera lub odpowiedzi wysyłanej przez aplikację. Wiele serwerów poczty e-mail, FTP i serwerów internetowych odpowiada na połączenie telnetowe z nazwą i wersją oprogramowania. To pomaga hakerowi w znalezieniu odcisku palca systemu operacyjnego i oprogramowania. Na przykład serwer pocztowy Microsoft Exchange może być zainstalowany tylko w systemie Windows.

Aktywny stos odcisków palców jest najbardziej powszechną formą pobierania odcisków palców. Obejmuje wysyłanie danych do systemu, aby zobaczyć, jak system reaguje. Opiera się na tym, że różni dostawcy systemów operacyjnych implementują stos TCP w różny sposób, a odpowiedzi różnią się w zależności od systemu operacyjnego. Odpowiedzi są następnie porównywane z bazą danych w celu określenia systemu operacyjnego. Odciski palców aktywnych stosów są wykrywalne, ponieważ wielokrotnie próbują połączyć się z tym samym systemem docelowym.

Pasywne skanowanie odcisków palców jest skrępowane i polega na badaniu ruchu w sieci w celu określenia systemu operacyjnego. Wykorzystuje techniki snifowania zamiast technik skanowania. Skanowanie odcisków palców pasywnych zwykle nie jest wykrywane przez system IDS lub inny system bezpieczeństwa, ale jest mniej dokładne niż aktywne skanowanie odciski palców.

Rysowanie schematów sieci hostów narażonych na atak

Chociaż nie jest to cel , zrozumienie narzędzi używanych w kroku 6 metodologii skanowania - rysowanie diagramu sieciowego podatnych hostów - jest koniecznością. Wiele narzędzi do zarządzania siecią może pomóc Ci w tym kroku. Takie narzędzia są zwykle używane do zarządzania urządzeniami sieciowymi, ale mogą zostać zwrócone przeciwko administratorom bezpieczeństwa przez hakerów. SolarWinds Toolset, Queso, Harris Stat i Cheops to narzędzia do zarządzania siecią, które mogą być używane do wykrywania systemów operacyjnych, mapowania diagramów sieciowych, listowania usług działających w sieci, wykonywania ogólnego skanowania portów i tak dalej. Te narzędzia pokazują całe sieci w interfejsie GUI, w tym routery, serwery, hosty i zapory ogniowe. Większość z tych narzędzi umożliwia wykrywanie adresów IP, nazw hostów, usług, systemów operacyjnych i informacji o wersji. Netcraft i HTTrack to narzędzia odcisków palców systemu operacyjnego. Obie są używane do określenia numerów wersji oprogramowania systemu operacyjnego i serwera WWW. Netcraft to strona internetowa, która okresowo odpytuje serwery WWW w celu określenia wersji systemu operacyjnego i wersji oprogramowania serwera WWW. Netcraft może dostarczyć przydatnych

informacji, których haker może użyć do identyfikacji luk w oprogramowaniu serwera sieciowego. Ponadto, Netcraft ma pasek narzędzi antyphishingowy i narzędzie do weryfikacji serwera sieciowego, którego możesz użyć, aby upewnić się, że używasz rzeczywistego serwera internetowego, a nie sfałszowanego serwera WWW. W ćwiczeniu 3.3 pokazano, jak używać Netcraft do identyfikacji systemu operacyjnego lub serwera WWW. HTTrack porządkuje względną strukturę linków oryginalnej witryny. Otworzysz stronę lustrzanej witryny w przeglądarce, a następnie możesz przeglądać witrynę z linku do łącza tak, jakbyś przeglądał ją online. HTTrack może również aktualizować istniejącą witrynę lustrzaną i wznawiać przerywane pobieranie.

Ćwiczenie 3.3

Użyj Netcraft do identyfikacji systemu operacyjnego serwera WWW

1. Otwórz przeglądarkę internetową na stronie Netcraft, www.netcraft.com.

2. Wpisz nazwę strony w serwisie What's That Running? pole w lewym górnym rogu ekran.

3. Przewiń w dół do opcji Historia hostingu, aby sprawdzić, jakie działa oprogramowanie systemu operacyjnego i serwera WWW na serwerze.

Skanowanie anonimowo

Przygotowanie serwerów proxy jest ostatnim krokiem w metodologii skanowania. Serwer proxy to komputer, który działa jako pośrednik między hakerem a komputerem docelowym. Korzystanie z serwera proxy może pozwolić na to, aby haker stał się anonimowy w sieci. Haker najpierw nawiązuje połączenie z serwerem proxy, a następnie żąda połączenia z komputerem docelowym za pośrednictwem istniejącego połączenia z serwerem proxy. Zasadniczo proxy żąda dostępu do komputera docelowego, a nie do komputera hakera. Dzięki temu haker może surfować po sieci anonimowo lub w inny sposób ukrywać atak.

Narzędzia hakerskie

SocksChain to narzędzie, dzięki któremu haker może atakować za pośrednictwem łańcucha serwerów proxy. Głównym celem jest ukrywanie prawdziwego adresu IP hakera, a tym samym minimalizowanie szansy na wykrycie. Kiedy haker działa przez kilka serwerów proxy w szeregu, znacznie trudniej jest zlokalizować hakera. Śledzenie adresu IP atakującego przez logi kilku serwerów proxy jest skomplikowaną i żmudną pracą. Jeśli jeden z plików dziennika serwera proxy zostanie utracony lub niekompletny, łańcuch zostanie przerwany, a adres IP hakera pozostanie anonimowy.

Anonimizatory to usługi, które próbują sprawić, by surfowanie po sieci było anonimowe dzięki wykorzystaniu strony internetowej, która działa jako serwer proxy dla klienta WWW. Pierwsze narzędzie anonymizera zostało opracowane przez Anonymizer.com; został stworzony w 1997 roku przez Lance'a Cottrella. Anonimizator usuwa wszystkie informacje identyfikujące z komputerów użytkownika, podczas gdy użytkownik surfuje po Internecie, zapewniając tym samym prywatność użytkownika. Aby anonimowo odwiedzać stronę internetową, haker wprowadza adres strony internetowej do oprogramowania anonymizera, a oprogramowanie anonimizujące przesyła żądanie do wybranej witryny. Wszystkie żądania i strony internetowe są przesyłane za pośrednictwem witryny anonimizera, co utrudnia śledzenie faktycznego requestera strony internetowej. Użyj anonimowości, aby anonimowo surfować po Internecie

Ćwiczenie 3.4.

Korzystaj z anonimowości w celu surfowania po stronach internetowych anonimowo

1. Otwórz przeglądarkę internetową na stronie http://anonymouse.org i wybierz English u góry strony.

2. Wpisz adres strony w polu Enter Website Address i kliknij przycisk Surf Anonimowo

Działa to szczególnie dobrze, jeśli wiesz, że niektóre witryny są zablokowane.

Popularną metodą ominięcia zapory lub IDS jest tunelowanie zablokowanego protokołu (takiego jak SMTP) za pośrednictwem dozwolonego protokołu (takiego jak HTTP). Prawie wszystkie IDS i firewalle działają jako pośrednik między komputerem klienta a Internetem i przekazują tylko ruch zdefiniowany jako dozwolony. Większość firm zezwala na ruch HTTP, ponieważ zwykle jest to łagodny dostęp do sieci. Jednak haker używający narzędzia tunelowania HTTP może obalić proxy, ukrywając potencjalnie destrukcyjne protokoły, takie jak komunikatory lub czat, w niewinnie wyglądającym pakiecie protokołów

Narzędzia hakerskie

HTTPort, Tunneld i BackStealth to narzędzia do tunelowania ruchu przez HTTP. Pozwalają na ominięcie serwera proxy HTTP, który blokuje dostęp niektórych protokołów do Internetu. Te narzędzia umożliwiają użycie następujących potencjalnie niebezpiecznych protokołów oprogramowania zza serwera proxy HTTP:

* e-mail

* IRC

* ICQ

* News

* AIM

* FTP

Haker może podszyć się pod adres IP podczas skanowania systemów docelowych, aby zminimalizować ryzyko wykrycia. Jedną z wad podszywania się pod adres IP jest to, że sesja TCP nie może zostać pomyślnie zakończona. Routing źródłowy pozwala intruzowi określić trasę, którą pakiet przechodzi przez Internet. Może to również zminimalizować ryzyko wykrycia przez ominięcie IDS i zapór ogniowych, które mogą blokować lub wykrywać atak. Routing źródłowy wykorzystuje adres zwrotny w nagłówku IP, aby zwrócić pakiet na sfałszowany adres zamiast rzeczywistego adresu atakującego. Wykorzystanie routingu źródłowego do ominięcia IDS zostanie omówione bardziej szczegółowo w Części 13. Aby wykryć podszywanie się pod adresy IP, można porównać wartości TTL (Time to Live): TTL atakującego będzie inne niż rzeczywisty TTL adresu spoofowanego.

Enumeracja

Wyliczenie występuje po skanowaniu i jest procesem zbierania i kompilowania nazw użytkowników, nazw komputerów, zasobów sieciowych, udziałów i usług. Odnosi się również do aktywnej kwerendy lub łączenia się z systemem docelowym w celu pozyskania tych informacji. Hakerzy muszą być metodyczni w podejściu do hakowania. Poniższe kroki są przykładem tych, które może wykonać haker w ramach przygotowań do włamania do systemu docelowego:

1. Wyodrębnij nazwy użytkowników za pomocą wyliczenia.

2. Zbierz informacje o hoście za pomocą sesji zerowych.

3. Wykonaj wyliczanie systemu Windows za pomocą narzędzia SuperScan.

4. Uzyskaj konta użytkowników za pomocą narzędzia GetAcct.

5. Przeprowadź skanowanie portu SNMP

Celem wyliczenia jest zidentyfikowanie konta użytkownika lub konta systemowego do potencjalnego wykorzystania w hakowaniu systemu docelowego. Nie jest konieczne znalezienie konta administratora systemu, ponieważ większość uprawnień konta można eskalować, aby umożliwić kontu większy dostęp niż wcześniej przyznano. Wiele narzędzi hakerskich zostało zaprojektowanych do skanowania sieci IP w celu zlokalizowania nazwy NetBIOS Informacja. Dla każdego hosta odpowiadającego adres IP listy narzędzi, nazwa komputera NetBIOS, zalogowana nazwa użytkownika i informacje o adresie MAC. W domenie Windows 2000 wbudowany widok sieci narzędziowej może być używany do wyliczania NetBIOS. Aby wyliczyć nazwy NetBIOS za pomocą polecenia net view, wprowadź poniższe

w wierszu polecenia:

net view / domain

nbtstat -A IP address

Narzędzia hakerskie

DumpSec to narzędzie do wyliczania NetBIOS. Łączy się z systemem docelowym jako użytkownik zerowy za pomocą polecenia net use. Następnie wylicza użytkowników, grupy, uprawnienia NTFS i informacje o własności plików. Hiena jest narzędziem, które wylicza udziały NetBIOS i dodatkowo może wykorzystać lukę w luce sesji, aby połączyć się z systemem docelowym i zmienić ścieżkę udziału lub edytować rejestr. Narzędzie audytu SMB to narzędzie do sprawdzania haseł do wiadomości systemu Windows i serwera platformy blokowe (SMB). Windows używa SMB do komunikacji między klientem a serwer. Narzędzie inspekcji SMB może identyfikować nazwy użytkowników i łamać hasła systemu Windows. Narzędzie NetBIOS Auditing Tool to kolejne narzędzie do wyliczania NetBIOS. Służy do przeprowadzania różnych kontroli bezpieczeństwa na zdalnych serwerach z usługami udostępniania plików NetBIOS.

Null Sessions

Sesja zerowa ma miejsce, gdy logujesz się do systemu bez nazwy użytkownika lub hasła. Sesje zerowe NetBIOS są luką w zabezpieczeniach Common Internet File System (CIFS) lub SMB, w zależności od systemu operacyjnego. Gdy haker utworzy połączenie NetBIOS, używając sesji zerowej do systemu, będzie mógł łatwo uzyskać pełny zrzut wszystkich nazw użytkowników, grup, udziałów, uprawnień, zasad, usług i innych elementów za pomocą konta użytkownika Null. Standardy SMB i NetBIOS w systemie Windows obejmują interfejsy API, które zwracają informacje o systemie za pośrednictwem portu TCP 139. Jedną z metod podłączenia sesji zerowej NetBIOS do systemu Windows jest wykorzystanie ukrytego udziału komunikacji między procesami (IPC $). Ten ukryty udział jest dostępny przy użyciu polecenia net use . Jak wspomniano wcześniej, polecenie net use jest wbudowanym poleceniem Windows, które łączy się z udziałem na innym komputerze. Puste cudzysłowy ("") oznaczają, że chcesz się połączyć bez nazwy użytkownika i hasła. Aby ustawić sesję null NetBIOS w systemie o adresie IP 192.21.7.1 z wbudowanym anonimowym kontem użytkownika i pustym hasłem przy użyciu polecenia net use, składnia jest następująca:

C: \>net use \\ 192.21.7.1 \ IPC $ "" / u: ""

Po pomyślnym zakończeniu komendy net use haker ma kanał, na którym można użyć innych narzędzi i technik hakerskich. Jako etyczny haker musisz wiedzieć, jak bronić się przed wyliczeniami NetBIOS i sesjami zerowymi. Omówimy to w następnej sekcji.

Wyliczanie NetBIOS i przeciwdziałanie sesji zerowej

Sesja zerowa NetBIOS używa określonych numerów portów na komputerze docelowym. Sesje zerowe wymagają dostępu do portów TCP 135, 137,139 i / lub 445. Jednym ze środków zaradczych jest zamknięcie tych portów w systemie docelowym. Można to osiągnąć, wyłączając usługi SMB na poszczególnych hostach, odrywając klienta TCP / IP WINS od interfejsu we właściwościach połączenia sieciowego. Aby wdrożyć ten środek zaradczy, wykonaj następujące kroki:

1. Otwórz właściwości połączenia sieciowego.

2. Kliknij TCP / IP, a następnie przycisk Właściwości.

3. Kliknij przycisk Zaawansowane.

4. Na karcie WINS wybierz opcję Wyłącz NetBIOS przez TCP / IP.

Administrator bezpieczeństwa może także edytować rejestr bezpośrednio, aby ograniczyć anonimowość użytkownik z logowania. Aby wdrożyć ten środek zaradczy, wykonaj następujące kroki:

1. Otwórz regedt32 i przejdź do HKLM \ SYSTEM \ CurrentControlSet \ LSA.

2. Wybierz Edycja ⇨ Dodaj wartość. Wprowadź następujące wartości:

* Nazwa wartości: RestrictAnonymous

* Typ danych : REG_WORD

* Wartość: 2

Wreszcie, system można uaktualnić do systemu Windows XP i najnowszych zabezpieczeń firmy Microsoft za pomocą łatki, które zmniejszają podatność na sesję o zerowej wartości NetBIOS.

Wyliczanie SNMP

Wyliczanie SNMP to proces używania protokołu SNMP do wyliczania kont użytkowników w systemie docelowym. SNMP wykorzystuje dwa główne typy komponentów oprogramowania do komunikacji: agenta SNMP, który znajduje się na urządzeniu sieciowym, oraz stację zarządzającą SNMP, która komunikuje się z agentem. Prawie wszystkie urządzenia infrastruktury sieciowej, takie jak routery i przełączniki, w tym systemy Windows, zawierają agenta SNMP do zarządzania systemem lub urządzeniem. Stacja zarządzania SNMP wysyła żądania do agentów, a agenci odsyłają odpowiedzi. Żądania odpowiedzi odnoszą się do zmiennych konfiguracyjnych dostępnych przez oprogramowanie agenta. Stacje zarządzania mogą również wysyłać żądania ustawiania wartości dla niektórych zmiennych. Pułapki informują stację zarządzającą o wystąpieniu znaczącego zdarzenia w oprogramowaniu agenta, na przykład w wyniku ponownego uruchomienia lub awarii interfejsu. Baza danych zarządzania (MIB) to baza danych zmiennych konfiguracyjnych, które znajdują się na urządzeniu sieciowym. Protokół SNMP ma dwa hasła, za pomocą których można uzyskać dostęp do agenta SNMP i skonfigurować go ze stacji zarządzania. Pierwszy nazywa się ciągiem społeczności read. To hasło umożliwia przeglądanie konfiguracji urządzenia lub systemu. Drugi nazywa się ciągiem społecznościowym do odczytu / zapisu; służy do zmiany lub edycji konfiguracji na urządzeniu. Ogólnie domyślny ciąg społeczności read jest publiczny, a domyślny ciąg społecznościowy do odczytu / zapisu jest prywatny. Typowa luka w zabezpieczeniach występuje wtedy, gdy łańcuchy społeczności pozostają w domyślnych ustawieniach: haker może używać tych domyślnych haseł do przeglądania lub zmiany konfiguracji urządzenia.

Narzędzia hakerskie

SNMPUtil i IP Network Browser to narzędzia do wyliczania SNMP. SNMPUtil zbiera informacje o kontach użytkowników Windows za pośrednictwem SNMP w systemach Windows. Niektóre informacje - takie jak tabele routingu, tabele ARP, adresy IP, adresy MAC, porty otwarte TCP i UDP, konta użytkowników i udziały - można odczytać z systemu Windows, w którym włączono SNMP za pomocą narzędzi SNMPUtil. Przeglądarka sieci IP z zestawu narzędzi SolarWinds również używa protokołu SNMP do gromadzenia dodatkowych informacji o urządzeniu, które ma agenta SNMP.

Przeciwdziałania wyliczeniom SNMP

Najprostszym sposobem zapobiegania wyliczaniu SNMP jest usunięcie agenta SNMP z potencjalnych systemów docelowych lub wyłączenie usługi SNMP. Jeśli wyłączenie SNMP nie jest opcją, zmień domyślne nazwy wspólnoty odczytu i zapisu / odczytu. Ponadto administrator może wdrożyć opcję zabezpieczeń Zasad grupowych Dodatkowe ograniczenia dotyczące połączeń anonimowych, które ograniczają połączenia SNMP.

Zasady grupy są implementowane na kontrolerze domeny Windows. Administratorzy sieci powinni wiedzieć, jak to zrobić.

Strefa Przesyłania DNS Windows 2000

W domenie Windows 2000 klienci używają rekordów usług (SRV) do lokalizowania domeny Windows 2000 usługi, takie jak Active Directory i Kerberos. Oznacza to, że każdy system Windows 2000 jest aktywny Domena katalogu musi mieć serwer DNS, aby sieć działała prawidłowo. Prosty transfer strefy wykonywany za pomocą polecenia nslookup może wyliczyć wiele interesujące informacje o sieci. Polecenie do wyliczenia za pomocą polecenia nslookup następująco:

nslookup ls -d nazwa_domeny

W wynikach nslookup haker przygląda się następującym zapisom, ponieważ dostarczają dodatkowych informacji o usługach sieciowych:

* Usługa globalnego katalogu (_gc._tcp_)

* Kontrolery domeny (_ldap._tcp)

* Uwierzytelnianie Kerberos (_kerberos._tcp)

Jako środek zaradczy, strefy transferu mogą być blokowane we właściwościach systemu Windows Serwer DNS. Baza danych Active Directory jest oparta na protokole Lightweight Directory Access Protocol (LDAP). Pozwala to na wyliczenie istniejących użytkowników i grup w bazie danych przez proste zapytanie LDAP. Jedyną rzeczą wymaganą do wykonania tego wyliczenia jest utworzenie uwierzytelnionej sesji przez LDAP. Windows 2000. Klient LDAP systemu Windows 2000 o nazwie Active Directory. Narzędzie administracyjne (ldp.exe) łączy się z serwerem Active Directory i identyfikuje zawartość bazy danych. Możesz znaleźć plik ldp.exe na dysku CD z systemem Windows 2000 w katalogu Support \ Reskit \ Netmgmt \ Folder Dstool. Aby wykonać wyliczenie Active Directory, haker wykonuje następujące kroki:

1. Połącz się z dowolnym serwerem Active Directory, używając programu ldp.exe na porcie 389. Po nawiązaniu połączenia informacje o serwerze zostaną wyświetlone w prawym okienku.

2. W menu Połączenie wybierz Uwierzytelnij. Wpisz nazwę użytkownika, hasło i nazwę domeny w odpowiednich polach. Możesz użyć konta Gość lub dowolnego innego konta domeny.

3. Po pomyślnym uwierzytelnieniu wylicz użytkowników i wbudowane grupy, wybierając opcję Wyszukaj z menu Przeglądaj.

Narzędzia hakerskie

User2SID i SID2User są narzędziami wiersza polecenia, które wyszukują identyfikatory usług Windows (identyfikatory SID od wejścia użytkownika i odwrotnie). Enum to narzędzie do wyliczania wiersza poleceń. Używa sesji zerowych i może pobierać nazwy użytkowników, nazwy komputerów, udostępnienia, listy grup i członków, hasła i informacje o zasadach zabezpieczeń lokalnych. Enum jest również zdolny do ataków słownikowych na indywidualne konta. UserInfo to narzędzie wiersza poleceń, które służy do zbierania nazw użytkowników i może być również używane do tworzenia nowych kont użytkowników. GetAcct to narzędzie oparte na GUI, które wylicza konta użytkowników w systemie. Smbbf to narzędzie brute-force firmy SMB, które próbuje określić konta użytkowników i konta z pustymi hasłami.

Podsumowanie

Skanowanie i wyliczanie to kolejne kroki w procesie hakerskim po zakończeniu fazy gromadzenia informacji. Narzędzia do skanowania i wyliczania są najczęściej aktywnymi narzędziami do zbierania informacji i dlatego umożliwiają wykrycie hakera. Z tego powodu istnieje wiele narzędzi i technik, aby zminimalizować możliwość wykrywania i zmniejszyć prawdopodobieństwo zidentyfikowania hakera. To podczas fazy skanowania i wyliczania informacja o hoście i sieć docelowa została odkryta. Kolejnym krokiem jest wyliczenie informacji o hoście i sieci, aby rozpocząć hakowanie docelowego systemu lub sieci. Następny rozdział skupi się na hakowaniu systemu i uzyskaniu dostępu do systemu docelowego.

Do Zapamiętania!

* Poznałeś trzy rodzaje skanowania i skanowania środków zaradczych. Port, sieć i Analiza podatności na atak to trzy rodzaje skanowania. Zaimplementuj zapory ogniowe, które uniemożliwiają skanowanie systemów wewnętrznych, blokując skanowanie w pętli i narzędzia do skanowania portów, takie jak nmap. IDS i IPS mogą ostrzec administratora o skanie przeprowadzanym w sieci.

* Dowiedziałeś się, jak określić, które systemy są aktywne w sieci. Nauczyłeś się używać narzędzia zapytań ICMP do wykonywania komend ping do określenia, które systemy odpowiadają. Pętle przewijania mają ograniczenia, a niektóre systemy mogą nie odpowiadać na kwerendy ICMP.

*Wiesz, jak przeprowadzić skanowanie portów za pomocą nmap. Dowiedz się, jak przełączniki działają skanowanie nmap za pomocą polecenia nmap. Na przykład nmap -sS wykonuje skanowanie SYN.

* Zapoznałęś się z zastosowaniami i ograniczeniami różnych typów skanowania. Upewnij się, że jesteś obeznany z połączeniami TCP, SYN, NULL, IDLE, FIN i XMAS i kiedy należy używać każdego typu.

* Zapoznałeś się z procesem potrójnego uzgadniania TCP. Proces połączenia TCP rozpoczyna się od wysłania pakietu SYN do systemu docelowego. System docelowy odpowiada pakietem SYN + ACK, a system źródłowy odsyła pakiet ACK do celu. To kończy udane połączenie TCP.

* Poznałeśj zastosowania wybierania war-dialing. Wirtualne wybieranie numeru służy do testowania zdalnego systemu dostępu dial-in . Numery telefonów wybierane są losowo w celu uzyskania niezabezpieczonego połączenia modemowego i uzyskania dostępu do sieci.

* Dowiedziałeś się, jak wykonywać odciski palców w systemie operacyjnym za pomocą metod aktywnych i pasywnych. Aktywny odcisk palca oznacza wysłanie żądania do systemu, aby zobaczyć, jak

zareaguje (na przykład przechwytywanie banerów). Pasywny odcisk palca sprawdza ruch przesyłany do i z systemu w celu określenia systemu operacyjnego.

* Dowiedziałeś się, jak stać się anonimowym przy użyciu anonimizera, tunelowania HTTP i podszywania się pod IP. Użyj anonimizera strony internetowej, aby ukryć adres źródłowy, aby system surfował po Internecie wyglądał anonimowo. Tunelowanie HTTP i podszywanie się pod IP to dwie metody ukrywania adresu fizycznego lub protokołów używanych przez hakera. Są przydatne w unikaniu zapór ogniowych i zaciemnianiu tożsamości lub miejsca pobytu hakera.

* Dowiedziałeś się, jak wyliczyć konta użytkowników. Wyliczanie polega na tworzeniu aktywnych połączeń z systemami za pomocą luk w zabezpieczeniach SMB / CIFS lub NetBIOS i wysyłaniu zapytań do systemu w celu uzyskania informacji.

* Należy pamiętać o typie informacji, które można wyliczyć w systemie i środkach zaradczych związanych z wyliczaniem. Typ informacji wymienianych przez hakerów obejmuje zasoby sieciowe i udziały, użytkowników i grupy oraz aplikacje i banery. Użyj zapory do blokowania portów 135 i 139 lub załatuj rejestr, aby zapobiec sesjom zerowym. Wyłącz usługi SNMP lub zmień domyślne nazwy społeczności do odczytu i zapisu / odczytu.

* Zapoznałeś się z sesjami zerowymi. Łączenie się z systemem przy użyciu pustego hasła jest znane jako sesja zerowa. Sesje zerowe są często wykorzystywane przez hakerów do łączenia się z systemami docelowymi, a następnie do uruchamiania narzędzi wyliczeniowych w systemie.

* Poznałeś typy narzędzi do wyliczania i dowiedz się, jak zidentyfikować podatne konta. Wyliczenia NetBIOS i SNMP można wykonywać za pomocą narzędzi takich jak SNMPUtil i Enum. Narzędzia takie jak User2SID, SID2User i UserInfo mogą być używane do identyfikacji podatnych kont użytkowników.

* Dowiedziałeś się, jak wykonać transfer strefy DNS na komputerach z systemem Windows 2000. NSlookup może służyć do wykonywania transferu strefy DNS