WYLICZENIE

Wyliczenie przenosi skanowanie portów na wyższy poziom. Teraz, gdy wiesz, jak wykrywać działające systemy w sieci, kolejne kroki obejmują sprawdzenie, jakie zasoby są współdzielone w systemach, odkrycie kont logowania i haseł oraz uzyskanie dostępu do zasobów sieciowych. Wyliczenie obejmuje połączenie z systemem zdalnym, a nie tylko sprawdzenie, czy system jest obecny w sieci. Hakerom nie wystarczy wiedza, że systemy komputerowe działają w sieci; ich celem jest znalezienie działających systemów i uzyskanie do nich dostępu. Dla testerów bezpieczeństwa wyliczanie jest bardziej inwazyjną częścią testowania i brak zgody właściciela sieci na ten krok może skutkować oskarżeniem o przestępstwo. Upewnij się, że posiadasz Zasady zaangażowania (ROE) i ewentualnie Wykaz prac (SOW), które jasno określają, jakie działania będziesz podejmować, i upewnij się, że uzyskałeś pisemną zgodę. Podczas wyliczania próbujesz odzyskać informacje i uzyskać dostęp do serwerów, korzystając z kont logowania pracowników firmy. W tych działaniach pomocna może być wiedza na temat systemów operacyjnych i sposobów przechowywania w nich informacji. Brak wiedzy, jak systemy Windows i Linux obsługują udziały i uprawnienia do plików, może utrudnić dostęp do informacji i znalezienie ewentualnych luk w zabezpieczeniach. W tym module poznasz podstawy różnych systemów operacyjnych i narzędzia do ich wyliczania. Niektóre z tych narzędzi zostały omówione wcześniej, inne są nowe, ale dzięki nim wyliczanie jest tak proste, jak wprowadzenie pojedynczego polecenia lub kliknięcie przycisku.

WPROWADZENIE DO WYLICZANIA

W poprzednich modułach widziałeś, jak wykonać transfer strefy, użyć polecenia dig i dowiedzieć się, jakie komputery znajdują się w sieci. Widziałeś także, jak używać narzędzi do skanowania portów (takich jak Nmap) do wykrywania urządzeń i usług w sieci. Kolejnym krokiem w testowaniu bezpieczeństwa jest wyliczenie, czyli proces wydobywania z sieci następujących informacji:

- Zasoby lub udziały w sieci
- Topologia i architektura sieci
- Nazwy użytkowników lub grupy przypisane w sieci
- Informacje o użytkownikach i czasie ostatniego logowania

Aby określić, jakie zasoby lub udziały są dostępne w sieci, testerzy bezpieczeństwa muszą najpierw przeprowadzić skanowanie portów i Footprinting, aby ustalić, jaki system operacyjny jest używany. Jeśli na przykład w sieci działa system operacyjny Windows, testerzy mogą używać określonych narzędzi do przeglądania udziałów i ewentualnego dostępu do zasobów. Jak wspomniano, wyliczanie jest bardziej inwazyjne, ponieważ nie tylko identyfikujesz zasób; próbujesz uzyskać do niego dostęp. Wyliczanie wykracza poza pasywne skanowanie sieci w celu znalezienia otwartych portów. Na przykład czasami proces ten polega na odgadywaniu haseł po ustaleniu nazwy użytkownika. W Ćwiczeniu 6-1 używasz NBTscan („NBT” oznacza NetBIOS przez TCP/IP), narzędzia do wyliczania systemów operacyjnych Windows, które jest częścią pakietu narzędzi bezpieczeństwa Kali Linux.

UWAGA: W przypadku niektórych ćwiczeń w tym module współpracujesz z partnerem w taki sposób, że jeden partner uruchamia system Windows, a drugi Linux. Powodem tego jest to, że w klasie działa kilka komputerów z systemem Windows, aby narzędzia wyliczające, z którymi pracujesz, mogły znaleźć systemy do wyliczenia. NetBIOS domyślnie nie działa w systemie Linux.

Korzystanie z narzędzia NBTscan

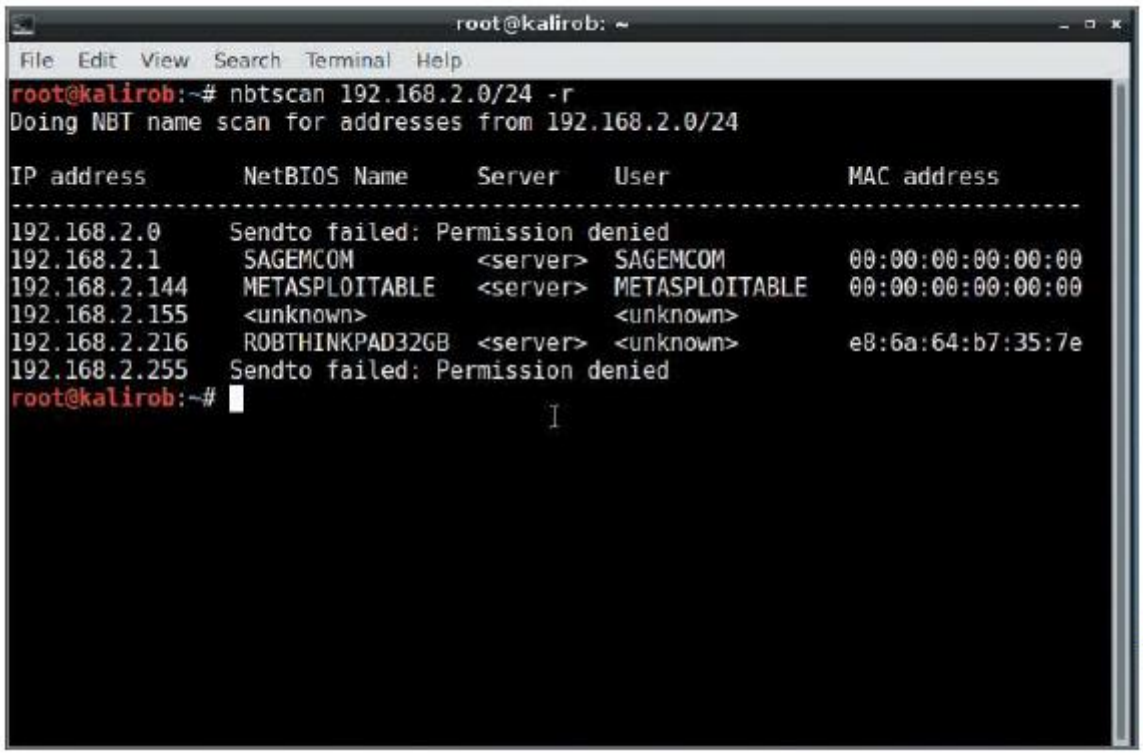
Wymagany czas: 5 minut

Cel: Nauczyć się korzystać z narzędzia NBTscan.

Opis: W tym ćwiczeniu współpracujesz z partnerem i używasz narzędzia NBTscan do znajdowania systemów z systemem NetBIOS.

1. Porozmawiaj ze swoim partnerem, aby zdecydować, kto uruchomi system Windows, a kto Kali Linux. Jeśli pracujesz sam, korzystaj z dwóch komputerów, rzeczywistego lub wirtualnego.

2. Otwórz powłokę terminala i wpisz nbtscan -h | less i naciśnij klawisz Enter, aby wyświetlić stronę pomocy. Korzystając z tych informacji, wprowadź polecenie NBTscan, aby przeskanować zakres adresów IP w sieci i sprawdzić, czy zostały zidentyfikowane jakieś komputery. Czy potrafisz zidentyfikować komputer z systemem Windows swojego partnera na wynikach? Rysunek przedstawia przykład danych wyjściowych komendy NBTscan.



Zwróć uwagę na komputery o nazwach etBIOS. Polecenie ujawnia również adresy MAC komputerów.

3. Zamknij Kali Linux i uruchom system Windows. Jeśli pracujesz z partnerem, powinien on uruchomić system Kali Linux i wykonać kroki 1 i 2.

4. Jeśli to konieczne, zamknij system Linux i uruchom system Windows, aby wykonać następną czynność.

WYLICZANIE SYSTEMÓW OPERACYJNYCH WINDOWS

Aby zrozumieć, w jaki sposób osoba atakująca może uzyskać dostęp do zasobów lub udziałów w sieci Windows, w tej sekcji przyjrzymy się krótko systemom operacyjnym Windows pod kątem ich powiązania z wyliczaniem. Domyślnie niewiele informacji można wyliczyć z systemów Windows po Windows 7.

Podstawy NetBIOS-u

Zanim nauczysz się wyliczać systemy Microsoft, musisz zapoznać się z podstawami działania sieciowego podstawowego systemu wejścia/wyjścia (NetBIOS). NetBIOS to interfejs programistyczny systemu Windows, który umożliwia komputerom komunikację poprzez sieć lokalną (LAN). Większość systemów operacyjnych Windows korzysta z protokołu NetBIOS do udostępniania plików i drukarek. NetBIOS nasłuchuje na portach UDP 137 (usługa nazw NetBIOS) i 138 (usługa datagramów NetBIOS) oraz porcie TCP 139 (usługa sesji NetBIOS). Udostępnianie plików i drukarek w systemie Windows wymaga również usługi wyższego poziomu o nazwie Server Message Block (SMB), która działa na platformie NetBIOS. W systemie Windows 2000 i nowszych wersjach protokół SMB nasłuchuje na porcie TCP 445 i nie musi używać protokołu NetBIOS przez protokół TCP/IP, chyba że wymagana jest obsługa starszych wersji systemu Windows.

UWAGA: Wyliczanie jest procesem odkrywania. Korzystanie z jednego narzędzia wyliczającego może prowadzić do odkrycia, które skieruje Cię do użycia innego narzędzia wyliczającego. Na przykład, jeśli użyłeś Nmapa i dowiedziałeś się, że urządzenie ma otwarte porty UPD 137 i 138 oraz port TCP 139 (wszystkie porty NetBIOS), możesz użyć narzędzia wyliczającego NetBIOS, takiego jak NBTscan, aby zobaczyć, czego więcej możesz się dowiedzieć na ten temat to urządzenie.

Nazwy komputerów przypisywane systemom Windows nazywane są nazwami NetBIOS i mają maksymalnie 16 znaków; ostatni znak jest zarezerwowany dla liczby szesnastkowej (00 do FF), która identyfikuje usługę uruchomioną na komputerze. Dlatego w nazwie komputera można użyć tylko 15 znaków, a system NetBIOS automatycznie dodaje ostatni znak w celu zidentyfikowania usługi zarejestrowanej w systemie operacyjnym. Na przykład, jeśli na komputerze działa usługa Serwer, system operacyjny przechowuje te informacje w tabeli NetBIOS. Nazwa NetBIOS musi być unikalna w sieci. Nie musisz zapamiętywać wszystkich tych przyrostków, ale pamiętaj, że niektóre identyfikują komputer lub serwer jako samodzielny komputer lub kontroler domeny. Hakerzy często wkładają więcej wysiłku w atakowanie komputerów zidentyfikowanych jako kontrolery domeny, ponieważ systemy te przechowują więcej informacji, w tym nazwy logowania kont użytkowników i zasoby sieciowe. Aby znaleźć bardziej obszerną listę sufiksów NetBIOS, można przeprowadzić wyszukiwanie w Internecie.

Nazwa NetBIOS Sufiks Opis

<nazwa komputera> : 00 : Usługa Stacja robocza zarejestrowała nazwę komputera (zwaną także nazwą NetBIOS).

<nazwa komputera> : 20 : Zarejestrowany przez usługę Serwera. Aby można było udostępniać drukarki lub pliki, na komputerze musi być uruchomiona ta usługa.

<nazwa komputera>: 22: Zarejestrowany w usłudze Microsoft Exchange Interchange.

<nazwa komputera> : 23 :- Zarejestrowany w usłudze Microsoft Exchange Store. Sklep to miejsce, w którym przechowywane są skrzynki pocztowe i foldery publiczne.

<nazwa komputera>: 24: Zarejestrowany w usłudze Microsoft Exchange Directory.

<nazwa komputera>: 87: Oznacza, że na tym komputerze działa program Microsoft Exchange Message Transfer Agent (MTA).

<nazwa domeny> : 00: Wskazuje, że system nazw domen (DNS) jest uruchomiony.

<nazwa domeny>: 1C: Identyfikuje komputer jako kontroler domeny.

<iNet~Services> :1C: Wskazuje, że IIS jest uruchomiony.

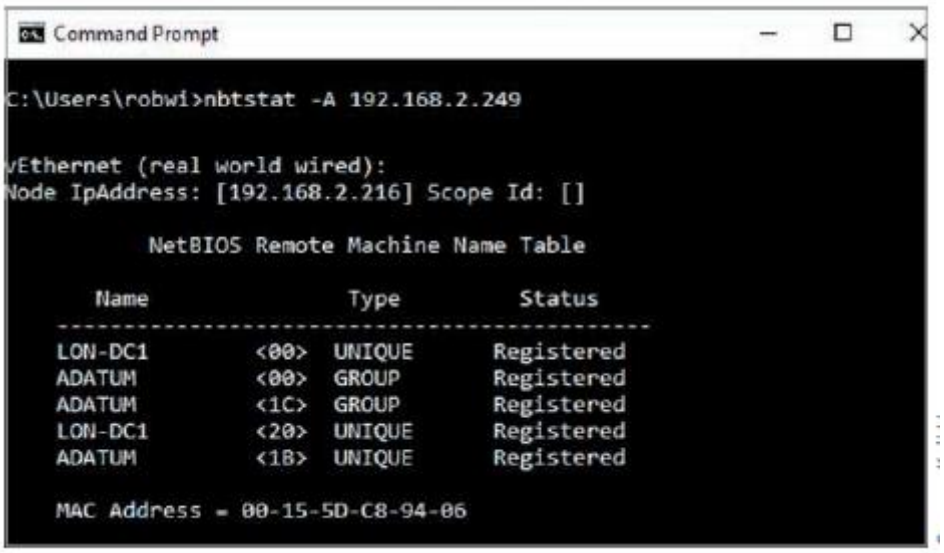
<IS~nazwa komputera> : 00 : Wskazuje również, że usługi IIS są uruchomione.

Sesje zerowe NetBIOS

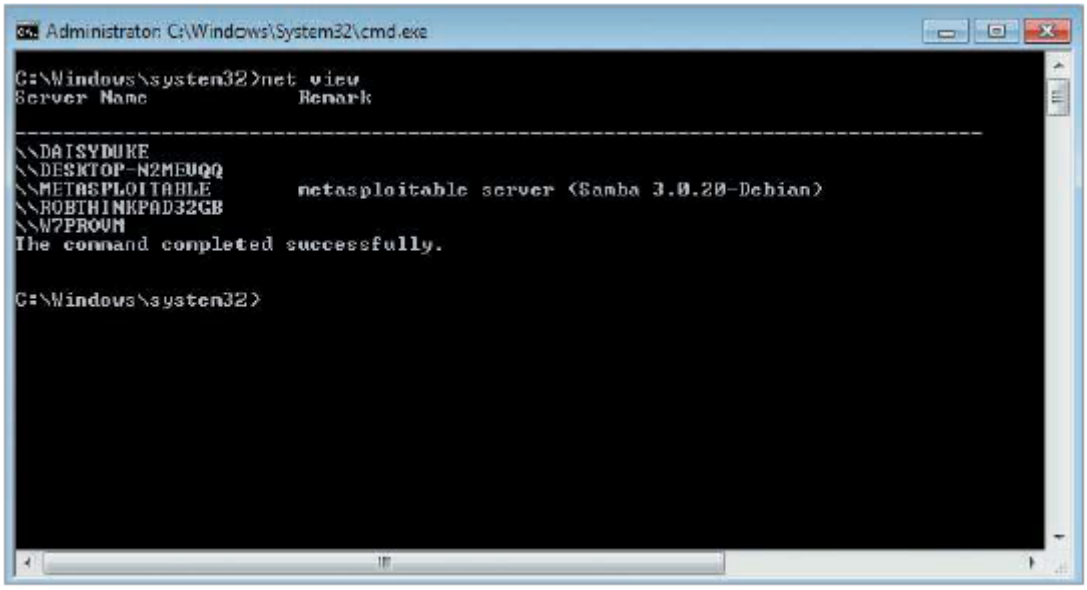
Historycznie rzecz biorąc, jedną z największych luk w zabezpieczeniach systemów NetBIOS jest sesja zerowa, czyli nieuwierzytelnione połączenie z komputerem z systemem Windows, które nie wykorzystuje wartości logowania i hasła. Wiele narzędzi wyliczeniowych omawianych w tym module ustanawia sesję zerową w celu zebrania informacji, takich jak konta logowania, członkostwo w grupach i udziały plików z zaatakowanego komputera. Luka ta istnieje już od ponad dziesięciu lat i nadal występuje w systemie Windows XP. Sesje zerowe zostały domyślnie wyłączone w systemie Windows Server 2003, chociaż administratorzy mogą je włączyć, jeśli z jakiegoś powodu są potrzebne. W systemach Windows Vista i Server 2008 sesje zerowe nie są dostępne i nie mogą zostać włączone nawet przez administratorów. Możesz zapytać: „Dlaczego mówimy o tych starożytnych systemach operacyjnych? „Kto już używa Windowsa XP?" Byłbyś zaskoczony. Jeśli jako tester penetracji znajdziesz starszy system operacyjny, właśnie odkryłeś poważną lukę w zabezpieczeniach, ponieważ te systemy operacyjne nie są już obsługiwane i nie otrzymują aktualizacji zabezpieczeń. Twoje działania obejmują aktualizację systemu operacyjnego, izolowanie podatnego na ataki starego systemu operacyjnego, tak aby nie był podłączony do żadnych sieci, lub likwidację systemu.

Narzędzia wyliczania NetBIOS

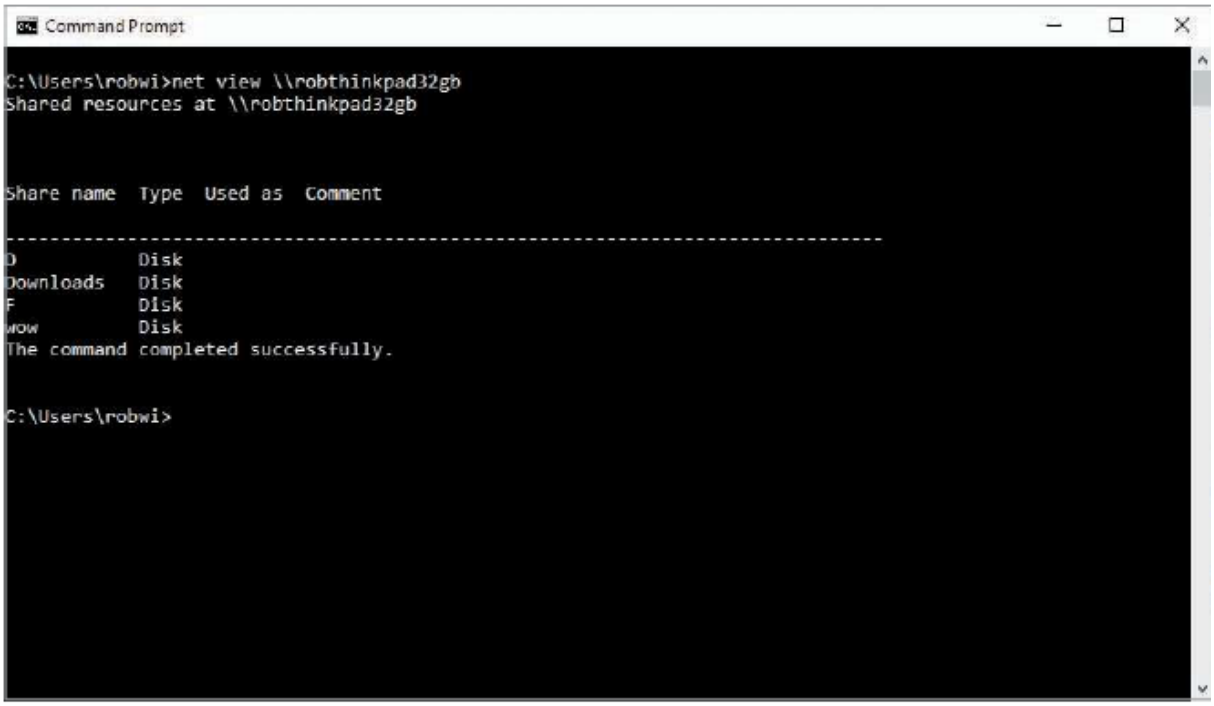
Polecenie nbtstat to potężne narzędzie wyliczające dostępne w systemie Windows. Aby wyświetlić tabelę NetBIOS, należy wydać polecenie nbtstat-a Adres IP. (Jeśli chcesz uruchomić Nbtstat lokalnie, poleceniem jest nbtstat-s.) Rysunek przedstawia wpis LON-DC1.



Liczba 20 oznacza usługę serwera działającą na komputerze LON-DC1. Tabela NetBIOS pokazuje również, że ADATUM jest kontrolerem domeny, na co wskazuje przyrostek 1C. Innym wbudowanym narzędziem systemu Windows jest polecenie net iew, które umożliwia szybkie sprawdzenie, czy istnieją jakieś udostępnione zasoby na komputerze lub serwerze. Aby wyświetlić składnię tego polecenia, wpisz net view ?. Za pomocą polecenia net view osoba atakująca może przeglądać zdalne udziały, jak pokazano na rysunku .



Możesz także użyć adresu IP komputerów odkrytych za pomocą narzędzi do skanowania portów. Na przykład rysunek przedstawia polecenie używane na zdalnym komputerze z systemem Windows 10.



Wyświetlana jest nazwa udziału o nazwie wow. Kolejnym poleceniem, którego osoba atakująca może użyć przeciwko temu komputerowi, jest \\robthinkpad32gb\wow, aby zbadać udostępniony dysk i wyszukać interesujące pliki. Chociaż możesz pobrać lub kupić narzędzia do wyliczania, powinieneś nauczyć się korzystać z narzędzi dostępnych w systemie Windows. Proste narzędzie wiersza poleceń może podać nazwę zalogowanego użytkownika, a odgadnięcie hasła tego użytkownika może zapewnić szybki dostęp do systemu. Wiele programów do łamania haseł może ustalić hasło w ciągu kilku sekund. Szybkie wyszukiwanie w Internecie odkryje wiele bezpłatnych programów do łamania haseł, które możesz wypróbować. Jednak testerzy bezpieczeństwa często potrafią odgadnąć hasła bez konieczności korzystania ze specjalnego programu, ponieważ niektórzy użytkownicy nieostrożnie tworzą hasła. Na przykład wielu użytkowników, pomimo wytycznych zawartych w polityce bezpieczeństwa firmy, używa

prostych haseł, takich jak „hasło” lub „p@$$w0rd”. Niektóre systemy mają także domyślne dane logowania, których użytkownicy często nie zmieniają, np. nazwę użytkownika „admin” z hasłem, które również brzmi „admin”. Listy domyślnych danych uwierzytelniających dla różnych urządzeń można znaleźć w Internecie. Wiele wspomnianych wcześniej programów do łamania haseł może używać brutalnej siły i próbować tysięcy logowań przy użyciu słowników zawierających tysiące haseł. Słowniki te obejmują dobrze znane, słabe hasła (takie jak hasło 1234) i dobrze znane domyślne poświadczenia.

Korzystanie z wbudowanych narzędzi NetBIOS systemu Windows

Wymagany czas: 30 minut

Cel: Naucz się korzystać z poleceń Windows Nbtstat, Net view i Net use.

Opis: W tym ćwiczeniu współpracujesz z partnerem w celu sprawdzenia narzędzi systemu Windows do przeglądania usług i udziałów NetBIOS. (Jeśli pracujesz sam, użyj dwóch komputerów, rzeczywistego lub wirtualnego.) Po użyciu polecenia Nbtstat w celu wykrycia komputera lub serwera sieciowego udostępniającego zasób, użyj poleceń Widok sieci i Użyj sieci, aby wyliczyć te udostępnione zasoby i ewentualnie uzyskać do nich dostęp z komputera.

1. Uruchom komputer i zaloguj się do systemu Windows, jeśli to konieczne.

2. Kliknij prawym przyciskiem myszy Start, a następnie kliknij Eksplorator plików. Kliknij opcję Ten komputer w lewym okienku, kliknij dwukrotnie opcję Dysk lokalny (C:) (lub inną nazwę dysku twardego), kliknij kartę Strona główna na wstążce (jeśli to konieczne), a następnie kliknij opcję Nowy folder. Wpisz YourFirstName jako nazwę folderu i naciśnij klawisz Enter.

UWAGA: Twoje imię jest symbolem zastępczym używanym w następujących poleceniach; zamiast tego używaj swojego prawdziwego imienia. (Jeśli utworzysz folder o nazwie YourFirstName, nie ma problemu; po prostu zapamiętaj nazwę folderu.)

3. Kliknij prawym przyciskiem myszy utworzony folder, kliknij opcję Daj dostęp, a następnie kliknij Określone osoby. W oknie dialogowym Dostęp do sieci wpisz Wszyscy, kliknij Dodaj, a następnie kliknij Udostępnij. Kliknij Gotowe, aby zamknąć

Okno dialogowe Dostęp do sieci.

4. Otwórz okno wiersza poleceń, wpisz ipconfig i naciśnij Enter. Zapisz swój adres IP i przekaż go swojemu partnerowi.

UWAGA: W kolejnych krokach adres IP znaleziony w kroku 4 jest reprezentowany przez zmienną Partner’sIPaddress. Zamiast wpisywać adres IP partnera, wpisz adres IP udostępniony partnerowi, gdy zobaczysz tę zmienną w poleceniu.

5. W wierszu poleceń wpisz net view \\Adres IP partnera i naciśnij Enter. Co polecenie generuje jako wynik?

6. Wpisz wykorzystanie netto? i naciśnij Enter. Polecenie Net use służy do łączenia się z komputerem zawierającym udostępnione foldery lub pliki.

7. Wpisz net use \\Partner’sIPaddress\YourFirstName (zastępując Partner’sIPAddress rzeczywistym adresem IP, który udostępniłeś swojemu partnerowi, a YourFirstName nazwą utworzonego folderu) i naciśnij Enter. Jakie są rezultaty tego polecenia?

8. Wpisz nbtstat -aAdres IP Partnera i naciśnij Enter. Jakie są rezultaty tego polecenia?

9. Zamknij wszystkie otwarte okna i zdecyduj, który partner będzie uruchamiał Kali Linux w ramach następnej czynności.

Dodatkowe narzędzia wyliczania

Jak widziałeś, kilka wbudowanych narzędzi systemu Windows może pomóc w wyliczeniu systemów NetBIOS. W poniższym ćwiczeniu sprawdzisz kilka dodatkowych narzędzi do tego zadania. Jednym z takich narzędzi jest enum4linux, narzędzie do wyliczania informacji z systemów Windows i Samba. Jest napisany w Perlu i wykorzystuje narzędzia Samby: smbclient, rpclient, net i nmblookup. Ponieważ enum4linux jest napisany w języku Perl, należy go uruchomić w systemie obsługującym Perl, takim jak Kali Linux.

Korzystanie z narzędzi wyliczania systemu Windows

Wymagany czas: 30 minut

Cel: Nauczyć się korzystać z narzędzi do mapowania i wyliczania sieci systemu Windows.

Opis: W tym ćwiczeniu będziesz eksplorować i testować niektóre narzędzia wyliczające systemu Windows zawarte w Kali Linux. Podobnie jak w Zadaniu 6.1, jeden partner uruchomił system Windows, a drugi Kali Linux. (Jeśli pracujesz sam, użyj dwóch komputerów, rzeczywistego lub wirtualnego.)

1. Uruchom komputer w systemie Kali Linux.

2. Otwórz okno terminala, wpisz enum4linux –h i naciśnij klawisz Enter, aby wyświetlić szczegóły użycia enum4linux.

3. Użyj narzędzia, aby wyliczyć udziały systemu Windows swojego partnera: Wpisz enum4linux -S Adres IP partnera i naciśnij klawisz Enter. Jeśli enum4linux nie wyliczy udziałów, może to oznaczać, że system Windows 10 domyślnie wyłączył dla gości zdalny dostęp do udziałów na liście. Jeśli masz starszą wersję systemu Windows, prawdopodobnie zobaczysz wyniki. Jeśli Ćwiczenie 6-2 zadziałało, komputer Twojego partnera prawdopodobnie został dodany do „Grupy domowej”. (Przeszukaj Internet, aby dowiedzieć się więcej o Windows HomeGroup.) Nowoczesne wersje systemu Windows prawie nie dostarczają żadnych informacji do enum4linux. To narzędzie jest bardziej skuteczne w przypadku starszych wersji systemu Windows.

4. Kliknij przycisk Aplikacje, a następnie kliknij 01 - Gromadzenie informacji, aby wyświetlić inne dostępne narzędzia

5. Poświęć kilka minut na zapoznanie się z funkcjami niektórych z tych narzędzi. Nie wahaj się eksperymentować lub przeszukaj Internet, aby uzyskać więcej informacji. Czy oprócz enum4linux i Nmap są jakieś inne narzędzia odpowiednie do wyliczania systemów Windows?

6. Zamień komputery ze swoim partnerem, a tę czynność powinien wykonać ten, który wcześniej korzystał z systemu Windows. Kiedy skończysz, upewnij się, że oba komputery są uruchomione w systemie Kali Linux w celu wykonania następnej czynności.

DumpSec

DumpSec to popularne narzędzie wyliczające dla systemów Windows NT, 2000 i XP. Nie działa dobrze w nowszych wersjach systemu Windows. Podczas wyliczania możesz natknąć się na starsze systemy Windows NT, 2000 lub XP, w których DumpSec może być przydatny. Jest produkowany przez firmę Foundstone, Inc. i można go pobrać ze strony www.systemtools.com/somarsoft/index.html. Informacje, które możesz zebrać za pomocą tego narzędzia, są niesamowite. Na przykład po połączeniu

się z serwerem Windows możesz pobrać — lub, jak to się nazywa w DumpSec, „zrzucić” — następujące informacje:

• Zezwolenia na udziały

• Uprawnienia dla drukarek

• Uprawnienia do Rejestru

• Użytkownicy w formacie kolumny lub tabeli

• Polityki (takie jak zasady lokalne, domenowe i grupowe)

• Prawa

• Usługi

Hyena

Hyena, dostępna pod adresem www.systemtools.com, to doskonałe narzędzie GUI do zarządzania i zabezpieczania systemów operacyjnych Windows. Interfejs jest łatwy w użyciu i zapewnia specjalistom ds. bezpieczeństwa mnóstwo informacji. Jest to narzędzie płatne, ale ma bezpłatną wersję próbną, z którą możesz eksperymentować. Możesz użyć Hieny, aby sprawdzić udziały i nazwy logowania użytkowników dla serwerów Windows i kontrolerów domen. Jeśli w sieci znajdują się jakieś domeny lub grupy robocze, to narzędzie również je wyświetla. Hiena może również wyświetlić graficzną reprezentację następujących obszarów:

• Usługi terminalowe Microsoft

• Sieć Microsoft Windows

• Sieć klienta internetowego

• Użytkownicy i grupy

Nessus i OpenVAS (aka Asystent Bezpieczeństwa Greenbone)

Być może znasz już narzędzia OpenVAS lub Greenbone Security Assistant (GSA) i Nessus. GSA działa w trybie klient/serwer i jest otwartym następcą Nessusa, popularnego narzędzia do identyfikowania luk w zabezpieczeniach. Zarówno Nessus, jak i OpenVAS są kompatybilne z Kali Linux i łatwe w instalacji. Najnowszą wersję Nessus Essentials dla systemów Windows, Linux i macOS można pobrać ze strony www.tenable.com. Pamiętaj, że Nessus Essentials ma wszystkie funkcje Nessus Professional, ale ma ograniczoną liczbę adresów IP, które możesz skanować. Instrukcje instalacji OpenVAS dla Kali Linux można znaleźć na stronie https://linuxhint.com/install-openvaskali-linux. Proces instalacji OpenVAS często się zmienia. Aby znaleźć najnowsze wskazówki, konieczne może być przeszukanie Internetu. W większości przypadków podczas wyliczania systemów można używać Nessusa lub OpenVAS zamiennie. Na przykład rysunek 6-9 przedstawia OpenVAS zgłaszający szczegóły luki w zabezpieczeniach „SSH Brute Force Logins with Default Credentials”. OpenVAS mógł zalogować się przez SSH przy użyciu znanych domyślnych poświadczeń, co stanowi zagrożenie bezpieczeństwa. Sugerowanym rozwiązaniem jest „Zmień hasło tak szybko, jak to możliwe”. OpenVAS wyliczył cel i odkrył, że działa na nim usługa SSH. Usługa SSH jest podatna na ataki. Poniższe rysunki przedstawiają przykłady wykorzystania Nessusa. Powinieneś zapoznać się z Nessusem, ponieważ wiele firm publicznych i prywatnych korzysta z niego podczas przeprowadzania testów bezpieczeństwa. Instalacja Nessusa jest

łatwa, a konfiguracja zajmuje kilka minut. To narzędzie może się przydać, gdy trzeba wyliczyć różne systemy operacyjne w dużej sieci. Dostęp do Nessusa można uzyskać poprzez interfejs sieciowy poprzez port 8834. Po przejściu do interfejsu sieciowego Nessus i uwierzytelnieniu otwiera się strona Skanowania pokazana na rysunku 6.10. Na tym ekranie możesz tworzyć, edytować i usuwać skany. Jeśli klikniesz przycisk Nowe skanowanie, możesz wybrać szablon skanowania odpowiedni do Twoich celów. Kilka kolejnych figurek przedstawia Nessusa w akcji. Nessus identyfikuje nazwę komputera jako W7PROVM, a nazwę grupy roboczej lub domeny jako WORKGROUP. Informacje te mogą być przydatne w przypadku późniejszych ataków. Dodatkowe skanowanie Nessusa w celu wyliczenia udziałów SMB dostarczyło listę folderów dostępnych za pośrednictwem protokołu SMB . Dostęp do folderów dostępnych za pośrednictwem protokołu SMB można uzyskać zdalnie przez sieć. Hakerzy mogą wykorzystać te informacje do przeprowadzenia ataków skierowanych na każdy z tych folderów. Jako tester penetracji możesz podjąć kroki, aby chronić te foldery przed hakerami, upewniając się, że te foldery dostępne dla SMB są zabezpieczone silnymi poświadczeniami i że wszelkie niepotrzebne udziały SBM zostały usunięte. Nessus jest również pomocny w identyfikowaniu systemu operacyjnego i dodatku Service Pack działającego na komputerze. System Windows 7 nie jest już obsługiwany przez firmę Microsoft, zatem obecność komputera z systemem Windows 7 w sieci stanowi poważny problem związany z bezpieczeństwem. Oprócz wyliczania systemów operacyjnych Windows, Nessus może również wyliczać systemy Linux i Unix.

WYLICZANIE *SYSTEM OPERACYJNY NIX

Spośród systemów operacyjnych omawianych w tym module UNIX jest najstarszym. Większość dostawców komputerów opracowała własne wersje tego popularnego systemu operacyjnego, ale ze względu na ograniczenia praw autorskich nie mogą używać „UNIX” w nazwach swoich produktów. (Tylko firma AT&T może używać nazwy UNIX.) Inne odmiany UNIX obejmują:

• Solaris (Sun Microsystems) i OpenSolaris

• HP-UX (Hewlett-Packard)

• Mac OS X i OpenDarwin, oparte na FreeBSD

• AIX (IBM)

• BSD UNIX (Uniwersytet Kalifornijski w Berkley)

• FreeBSD (UNIX oparty na BSD, opracowany przez autorów)

• OpenBSD (UNIX oparty na BSD, opracowany przez autorów)

• NetBSD (UNIX oparty na BSD, opracowany przez autorów)

• Linux, w tym następujące dystrybucje:

❍ Ubuntu (oparty na Debianie, sponsorowany przez Canonical)

❍ Kali Linux (oparty na Debianie)

❍ Red Hat Enterprise Linux (wydany komercyjnie przez firmę Red Hat)

❍ Fedora Linux (opracowana przez autorów i sponsorowana przez firmę Red Hat)

❍ Debian Linux (opracowany przez autorów)

❍ SUSE Linux (Micro Focus) i OpenSUSE

❍ Mandriva Linux (odległy komercyjny rozwidlenie Red Hata z 1990 r.)

❍ Slackware (najstarsza zachowana dystrybucja Linuksa)

Jak widać, wiele organizacji ma wersję UNIX. Linux, stworzony przez Linusa Torvaldsa, jest właśnie tym: odmianą UNIX-a pierwotnie zaprojektowaną dla niedrogich komputerów Intel. Biorąc pod uwagę wszystkie dostępne odmiany UNIX-a, nic dziwnego, że wielu profesjonalistów komputerowych używa tego systemu operacyjnego. Najnowsze wersje Linuksa są łatwiejsze w instalacji i konfiguracji oraz zawierają graficzne interfejsy użytkownika i przeglądarki internetowe, dzięki którym korzystanie z oprogramowania jest mniej skomplikowane. Dzięki Grand Unified Bootloader (GRUB) możesz uruchomić swój komputer stacjonarny lub laptop zarówno w systemie Windows, jak i Linux. Nawet początkujący użytkownicy komputerów mogą łatwo zainstalować najnowszą wersję. Większość dystrybucji Linuksa ma wersje Live CD/DVD lub pamięci USB, które można wypróbować bez instalowania ich na dysku twardym. Warianty Linuksa można również znaleźć działające na urządzeniach takich jak smartfony, komputery Apple, urządzenia Internetu rzeczy i urządzenia zabezpieczające sieć.

***nix enumeracja**

Starą, ale wciąż popularną usługą zarządzania siecią dla administratorów sieci jest Simple Network Management Protocol (SNMP), który umożliwia zdalną administrację. Usługę SNMP można uruchomić zarówno w systemie Windows, jak i *nix, chociaż w tej sekcji skupimy się na *nix. SNMP jest przydatny dla administratorów, którzy chcą zdalnie przeglądać statystyki systemu, numery wersji i inne szczegółowe informacje o hoście. Z tego powodu jest to również przydatne dla hakerów. Domyślnie usługa SNMP używa „publicznego” jako poświadczenia dla dostępu tylko do odczytu i „prywatnego” dla dostępu do odczytu i zapisu. SNMPWalk to narzędzie przydatne do zliczania hostów korzystających z protokołu SNMP w domyślnej konfiguracji. (Patrz rysunek 6-14). Jeśli atakujący znają architekturę procesora (zazwyczaj 32-bitową lub 64-bitową) i szczegółowy numer wersji zdalnego systemu operacyjnego, łatwiej będzie im znaleźć skuteczne exploity. Demon SNMP (snmpd) nasłuchuje na porcie UDP 161. SNMP często działa na sprzęcie sieciowym, takim jak routery, przełączniki i zapory ogniowe. Urządzenia te mają również systemy operacyjne, które mogą zawierać luki w zabezpieczeniach, które można wykorzystać. Nessus jest również pomocny w wyliczaniu *nix. Rysunek 6-15 pokazuje, co Nessus znalazł podczas skanowania systemu Ubuntu 15.10 Skanery podatności, takie jak Nessus i OpenVAS, są przydatne do wyliczania hostów *nix, ale proste narzędzia, takie jak skanowanie skryptów Nmap, mogą również pomóc atakującemu uzyskać informacje o zdalnych hostach *nix. Rysunek 6-16 pokazuje, co Nmap znalazł podczas skanowania systemu Ubuntu 15.10. Starszym, ale czasami przydatnym narzędziem do wyliczania zarówno dla testerów bezpieczeństwa, jak i hakerów, jest narzędzie Finger, które pozwala za pomocą jednego polecenia dowiedzieć się, kto jest zalogowany do *nix. System Finger jest zarówno klientem, jak i serwerem. Demon Finger (fingerd) nasłuchuje na porcie TCP 79.

Wyliczanie serwerów WWW *nix za pomocą Nmap

Wymagany czas: 30 minut

Cel: Naucz się korzystać z narzędzia Nmap na lokalnych i zdalnych systemach *nix.

Opis: W tym ćwiczeniu użyjesz polecenia Nmap, aby wyliczyć swój komputer i zobaczyć, w jaki sposób to potężne polecenie może zebrać informacje z systemu zdalnego. Dowiesz się także, jak uruchamiać i zatrzymywać usługi na komputerze lokalnym

UWAGA: w tym ćwiczeniu włączasz kilka usług, które mogą narazić komputer na ryzyko, jeśli nie podejmiesz odpowiednich środków ostrożności. Jeśli Twoja instalacja Kali nie ma możliwości logowania się na konto root, musisz zmienić hasło za pomocą polecenia passwd root. Umożliwi to logowanie roota..

1. Jeśli to konieczne, uruchom komputer w systemie Kali Linux i zaloguj się.

2. Większość usług Linuksa uruchamiana jest za pomocą serii skryptów przechowywanych w katalogu /etc/init.d/. Możesz wyświetlić zawartość tego folderu za pomocą następującego polecenia: ls /etc/init.d/.

3. Uruchom usługi ssh i samba na lokalnym hoście za pomocą następujących poleceń: /etc/init.d/ssh start i /etc/init.d/samba start.

4. Użyj Nmap, aby uruchomić skryptowe skanowanie hosta lokalnego (127.0.0.1). Rysunek 6-16 przedstawia przykład skanowania skryptowego Nmap. Jakie wyniki zostały zwrócone? Z jakiej wersji protokołu SSH korzysta Twój komputer? Jaka wersja Samby?

5. Czy te wersje SSH lub Samby mają jakieś luki w zabezpieczeniach?

6. Użyj następujących poleceń, aby zatrzymać włączone usługi: /etc/init.d/sshd stop i /etc/init.d/samba stop. Wyłącz komputer Kali Linux.

PODSUMOWANIE MODUŁÓW

• Wyliczanie to proces wyodrębniania nazw użytkowników, haseł i współdzielonych zasobów z systemu.

• Wyliczenie może zapewnić osobie atakującej wgląd we wrażliwe obszary sieci, systemy ze starym oprogramowaniem, a nawet proste błędne konfiguracje, które osoba atakująca może wykorzystać.

• Wyliczanie celów systemu Windows można wykonać za pomocą wbudowanych narzędzi systemu Windows, takich jak polecenia Nbtstat, Net view i Net use, lub za pomocą wielu innych narzędzi. Narzędzia takie jak enum4linux mogą wyliczać system Windows z różnych wersji *nix. Nowsze wersje systemu Windows są trudniejsze do wyliczenia ze względu na postęp w zakresie zabezpieczeń systemu Windows z biegiem czasu.

• Wyliczanie systemów *nix można wykonać za pomocą narzędzi używanych do wyliczania innych systemów operacyjnych, takich jak Nessus i jego potomek o otwartym kodzie źródłowym, OpenVAS.

• Protokołu SNMP można używać do wyliczania hostów *nix i Windows, na których działa usługa/demon SNMP z domyślną konfiguracją.