SKANOWANIE PORTÓW

Skanowanie portów, nazywane również skanowaniem usług, to proces badania zakresu adresów IP w celu ustalenia, jakie usługi są uruchomione w sieci. Otwarte porty na komputerze mogą identyfikować usługi na nim uruchomione. Na przykład protokół HTTP używa portu 80 do łączenia się z usługą internetową. Zamiast pingować każdy adres IP w zakresie adresów i czekać na odpowiedź ICMP Echo Reply (typ 0), aby sprawdzić, czy można dotrzeć do komputera, możesz użyć narzędzi skanujących, aby uprościć tę procedurę. W końcu pingowanie kilku tysięcy adresów IP ręcznie jest czasochłonne. Narzędzia do skanowania portów mogą być złożone, dlatego musisz poświęcić czas na poznanie ich mocnych i słabych stron oraz zrozumienie, jak i kiedy należy ich używać. W tym module przyjrzysz się narzędziom do skanowania portów, które umożliwiają identyfikację usług uruchomionych w sieci i wykorzystanie tej wiedzy do przeprowadzenia testu bezpieczeństwa. Ponadto zobaczysz, jak używać skryptów powłoki do automatyzacji przeszukiwania pingów i innych zadań testowania bezpieczeństwa.

WPROWADZENIE DO SKANOWANIA PORTÓW

Przypomnij sobie, że możesz wykonać transfer strefy za pomocą polecenia dig, aby określić adresy IP sieci. Załóżmy, że transfer strefy wskazuje, że firma używa podsieciowego adresu klasy C ze 126 dostępnymi adresami IP hosta. Jak sprawdzić, czy wszystkie te adresy są używane przez komputery, które są uruchomione i działają? Używasz skanera portów, aby pingować zakres adresów IP, które odkryłeś. Ważniejszym pytaniem, jakie powinien zadać tester bezpieczeństwa, jest „Jakie usługi są uruchomione na zidentyfikowanych komputerach?” Skanowanie portów to metoda ustalania, jakie usługi oferuje komputer hosta. Na przykład, jeśli serwer hostuje witrynę internetową, czy prawdopodobne jest, że serwer ma otwarty port 443, a może port 80? Czy któraś z usług jest podatna na ataki lub exploity? Czy któraś z usług nie jest filtrowana przez zaporę, co umożliwia załadowanie trojana, który może wysyłać informacje z zaatakowanego komputera? Który komputer jest najbardziej podatny na atak? Wiesz już, jak wyszukiwać znane luki w zabezpieczeniach, korzystając ze stron internetowych Common Vulnerabilities and Exposures (https://cve.mitre.org) i US-CERT (www.us-cert.gov). Możesz również użyć narzędzi do skanowania portów, które identyfikują luki w zabezpieczeniach — na przykład Angry IP Scanner (angryip.org), bezpłatnego skanera portów z interfejsem GUI (patrz Rysunek 5-1). Za pomocą tego narzędzia atakujący może szybko zidentyfikować otwarty port, a następnie uruchomić exploit atakujący system. Jako tester bezpieczeństwa musisz wiedzieć, które porty atakują atakujący, aby móc je zamknąć i zabezpieczyć. Testerzy bezpieczeństwa muszą skanować wszystkie porty podczas przeprowadzania testu, a nie tylko dobrze znane porty. Wiele programów używa numerów portów spoza zakresu dobrze znanych portów. Na przykład TeamViewer, znany program do zdalnego sterowania komputerami PC, działa na portach 5938, 443 i 80. Haker, który odkryje, że port 5938 jest otwarty, może sprawdzić informacje na stronie internetowej CVE pod kątem możliwej luki w zabezpieczeniach TeamViewer. Po odkryciu otwartej usługi przez hakera znalezienie luki lub exploita nie jest trudne, szczególnie gdy systemy są nieaktualne i niezałatane.

BAJTY BEZPIECZEŃSTWA

Większość testerów bezpieczeństwa i hakerów twierdzi, że skanowanie portów jest legalne, ponieważ nie narusza prywatności innych; po prostu odkrywa, czy skanowana strona jest dostępna. Typowa analogia to osoba idąca ulicą i przekręcająca klamkę każdego domu po drodze. Jeśli drzwi się otworzą, osoba ta zauważa, że drzwi są otwarte i przechodzi do następnego domu. Oczywiście, wejście do domu jest przestępstwem w większości części świata, tak jak wejście do komputera lub systemu sieciowego bez zgody właściciela jest przestępstwem. Do tej pory nikt nie został skazany za samo skanowanie portów w Stanach Zjednoczonych, chociaż niektóre prawa przewidują ściganie za skanowanie, jeśli

spowoduje ono uszkodzenie lub stratę przekraczającą 5000 USD (Kodeks Stanów Zjednoczonych 18 1030).

Skanowanie portów pomaga odpowiedzieć na pytania dotyczące otwartych portów i usług, umożliwiając szybkie skanowanie tysięcy, a nawet dziesiątek tysięcy adresów IP. Wiele narzędzi do skanowania portów generuje raporty ze swoich ustaleń, a niektóre dają najlepsze szacunki dotyczące tego, który system operacyjny jest uruchomiony w systemie. Większość, jeśli nie wszystkie, programy skanujące zgłaszają otwarte porty, zamknięte porty i filtrowane porty w ciągu kilku sekund. Otwarty port umożliwia dostęp do aplikacji i może być podatny na ataki. Gdy serwer WWW musi komunikować się z aplikacjami lub innymi komputerami, na przykład, otwierany jest port 443. Zamknięty port nie zezwala na wejście ani dostęp do usługi. Na przykład, jeśli porty 443 i 80 są zamknięte na serwerze WWW, użytkownicy nie mogą uzyskać dostępu do witryn internetowych. Port zgłoszony jako filtrowany może wskazywać, że zapora jest używana do zezwalania na określony ruch do lub z sieci.

Rodzaje skanowania portów

Zanim zagłębisz się w narzędzia do skanowania portów, zapoznaj się z rodzajami skanowania, których można użyć do skanowania portów:

• Skanowanie SYN — w normalnej sesji TCP pakiet jest wysyłany do innego komputera z ustawioną flagą SYN. Komputer odbierający odsyła pakiet z ustawioną flagą SYN/ACK, co oznacza potwierdzenie. Następnie komputer wysyłający wysyła pakiet z ustawioną flagą ACK. Jeśli pakiet SYN jest wysyłany do zamkniętego portu, komputer odpowiada pakietem RST/ACK (reset/potwierdzenie). Jeśli komputer atakującego odbiera pakiet SYN/ACK, odpowiada szybko pakietem RST/ACK, zamykając sesję. Robi się to tak, aby nigdy nie nawiązano pełnego połączenia TCP i nie zarejestrowano go jako transakcji. W tym sensie jest to „ukryte". W końcu atakujący nie chcą, aby zarejestrowana transakcja pokazywała ich połączenie z zaatakowanym komputerem i zawierała ich adresy IP.

• Skanowanie połączeń — Ten typ skanowania opiera się na systemie operacyjnym atakowanego komputera, więc jest bardziej ryzykowny w użyciu. Skanowanie połączeń jest podobne do skanowania SYN, z tą różnicą, że wykonuje trzyetapowe uzgadnianie. Oznacza to, że atakowany komputer najprawdopodobniej rejestruje transakcję lub połączenie, wskazując, że sesja miała miejsce. Dlatego w przeciwieństwie do skanowania SYN, skanowanie połączeń nie jest ukryte i można je łatwo wykryć.

• Skanowanie NULL — W skanowaniu NULL wszystkie flagi pakietów są wyłączone. Zamknięty port odpowiada na skanowanie NULL pakietem RST, więc jeśli nie zostanie odebrany żaden pakiet, najlepszym przypuszczeniem jest to, że port jest otwarty. Jednak system Windows nie przestrzega standardu i może odpowiedzieć w nieoczekiwany sposób.

• Skanowanie XMAS — W tym typie skanowania ustawiane są flagi FIN, PSH i URG. Zamknięte porty odpowiadają na ten typ pakietu pakietem RST. Tego skanowania można użyć do określenia, które porty są otwarte. Na przykład atakujący może wysłać ten pakiet do portu 53 w systemie i sprawdzić, czy zwrócony zostanie pakiet RST. Jeśli nie, port DNS może być otwarty. Ponownie, system Windows nie stosuje się do standardu i losowo odpowiada na skanowanie XMAS.

• Skanowanie ACK — atakujący zazwyczaj używają skanowania ACK, aby ominąć zaporę lub inne urządzenie filtrujące. Urządzenie filtrujące szuka pakietu SYN, pierwszego pakietu w trzyetapowym uzgadnianiu, którego częścią był pakiet ACK. Zapamiętaj tę kolejność pakietów: SYN, SYN/ACK i ACK. Jeśli atakowany port zwróci pakiet RST, filtr pakietów został oszukany lub nie ma urządzenia filtrującego pakiety. W obu przypadkach atakowany port jest uważany za „niefiltrowany".

• Skanowanie FIN — w tym typie skanowania pakiet FIN jest wysyłany do komputera docelowego. Jeśli port jest zamknięty, wysyła on pakiet RST. Po zakończeniu trzyetapowego uzgadniania obie strony wysyłają pakiet FIN, aby zakończyć połączenie.

• Skanowanie UDP — w tym typie skanowania pakiet UDP jest wysyłany do komputera docelowego. Jeśli port odeśle komunikat ICMP „Port Unreachable", port jest zamykany. Ponownie, brak otrzymania tego komunikatu może oznaczać, że port jest otwarty, ale nie zawsze tak jest. Zapora sieciowa lub urządzenie filtrujące pakiety mogą podważyć Twoje założenia.

Komputer, który otrzymuje pakiet SYN od komputera zdalnego, odpowiada pakietem SYN/ACK, jeśli jego port jest otwarty. W przypadku trzyetapowego uzgadniania pakiet SYN jest wysyłany z jednego komputera, pakiet SYN/ACK jest wysyłany z komputera odbierającego do nadawcy, a na koniec nadawca wysyła pakiet ACK do komputera odbierającego. Jeśli port jest zamknięty i odbiera pakiet SYN, wysyła z powrotem pakiet RST/ACK. Określenie, czy port jest filtrowany, jest bardziej złożone. Wiele narzędzi skanujących, takich jak Nmap, wykorzystuje podejście oparte na najlepszym zgadywaniu. Oznacza to, że jeśli pakiet UDP nie otrzyma odpowiedzi z portu odbierającego, wiele narzędzi skanujących zgłasza, że port jest otwarty.

BAJTY BEZPIECZEŃSTWA

W Kanadzie pewien mężczyzna został uznany za winnego skanowania komputerów firmy. Firma oskarżyła go o wykorzystanie mikrowatów swojej energii elektrycznej do przeprowadzenia skanowania. Robienie tego bez zgody firmy było uważane za przestępstwo — drobne, owszem, ale skuteczne. Aby zachować bezpieczeństwo, zawsze uzyskaj pozwolenie od firmy, jeśli zamierzasz przeprowadzić intensywne skanowanie jej infrastruktury sieciowej. Jeśli skanowanie spowalnia ruch sieciowy, firma może argumentować, że przeprowadzono atak DoS niskiego poziomu, który jest nielegalny.

KORZYSTANIE Z NARZĘDZI DO SKANOWANIA PORTÓW

Dostępnych jest setki narzędzi do skanowania portów zarówno dla hakerów, jak i testerów bezpieczeństwa. Niektóre są komercyjne, a niektóre są darmowe lub mają otwarte oprogramowanie. Jak zdecydować, którego narzędzia użyć? Nie wszystkie są dokładne, dlatego zaleca się korzystanie z więcej niż jednego narzędzia do skanowania portów. Ponadto warto zapoznać się z różnymi narzędziami. Chociaż należy często ćwiczyć z narzędziem, aby zdobyć biegłość w jego używaniu, nie wpadnij w pułapkę polegającą na korzystaniu wyłącznie z jednego narzędzia.

Nmap

Oryginalnie napisany dla magazynu Phrack w 1997 roku przez Fyodora, Nmap stał się jednym z najpopularniejszych skanerów portów i stale dodaje nowe funkcje, takie jak wykrywanie systemu operacyjnego i szybkie skanowanie pingów z wieloma sondami. Nmap ma również interfejs użytkownika GUI o nazwie Zenmap, który ułatwia pracę ze złożonymi opcjami. Nmap był udoskonalany na przestrzeni lat, ponieważ, podobnie jak wiele innych narzędzi bezpieczeństwa, jest oprogramowaniem typu open source; w przypadku znalezienia błędów użytkownicy mogą zaproponować sugestie dotyczące ich usunięcia. Nmap jest często przywoływany w tym kursie, ponieważ jest obecnie standardowym narzędziem do skanowania portów dla profesjonalistów ds. bezpieczeństwa. Niezależnie od innych dostępnych narzędzi do skanowania portów, każdy tester bezpieczeństwa z odrobiną doświadczenia pracował z Nmap. Jako początkujący student możesz używać go w każdej części testu bezpieczeństwa lub penetracji, ale pamiętaj, aby rozwijać biegłość w różnych narzędziach.

BAJTY BEZPIECZEŃSTWA

Jak powie ci większość profesjonalistów od bezpieczeństwa, Hollywood rzadko pokazuje atakujących faktycznie włamujących się do systemu. Zazwyczaj używają programu GUI, gorączkowo klikają lub wpisują algorytm deszyfrujący. Wyjątkiem jest Matrix Reloaded. Główna bohaterka, Trinity, siedzi przy terminalu komputerowym i uruchamia Nmap. Odkrywa, że port 22 (SSH) jest otwarty, uruchamia exploit SSHv1 CRC32 (faktyczny błąd w SSH), który pozwala jej zmienić hasło roota na Z1ON0101, a następnie wyłącza sieć. Morał z tej historii? Poznaj swoje narzędzia i exploity, a możesz uratować świat.

Nie musisz zapamiętywać, jak każda flaga jest ustawiana podczas skanowania portów za pomocą Nmap. W rzeczywistości samo wpisanie polecenia nmap 193.145.85.2 01 skanuje typowe porty na komputerze o tym adresie IP. Jednak skanowanie portów może być złożonym procesem. Niektórzy atakujący chcą być ukryci przed urządzeniami sieciowymi lub systemami IDS, które rozpoznają nadmierną liczbę pingów lub pakietów wysyłanych do ich sieci, więc stosują ataki ukryte i ograniczają prędkość skanowania, aby utrudnić wykrycie ich działań. Oprócz tych technik atakujący może obrać za cel tylko kilka portów zamiast skanowania wszystkich typowych portów. W poniższych działaniach zapoznasz się z podstawowymi poleceniami Nmap, a następnie poznasz niektóre z bardziej złożonych opcji.

Aktywność 5-1: Poznawanie Nmap

Czas trwania: 30 minut

Cel: poznanie podstawowych poleceń i składni Nmap.

Opis: w tej aktywności używasz Nmap do wykonywania szybkich skanów sieci. Wysyłasz pakiet SYN do hosta w sieci atakującej, którą dostarczył Ci instruktor. W tym przykładzie adresy IP sieci atakującej to 136.142.35.137 do 136.142.35.140, ale zakres Twojego ataku może być inny. Upewnij się, że przestrzegasz zasad zaangażowania i nie wykonuj skanowania portów w żadnych systemach, które nie znajdują się w zakresie IP podanym przez instruktora.

1. Uruchom komputer w systemie Linux. Otwórz powłokę poleceń, klikając ikonę terminala na pasku zadań panelu. Wpisz nmap -h | less i naciśnij Enter, aby wyświetlić wszystkie dostępne polecenia Nmap. Możesz przewijać, aby przejrzeć parametry polecenia.

2. Po przejrzeniu parametrów zapisz trzy opcje, których można użyć z poleceniem Nmap, a następnie naciśnij q, aby wyjść z ekranu pomocy.

3. Aby wysłać pakiet SYN na adres IP w zakresie ataku, wpisz nmap -sS -v 136.142.35.137 i naciśnij Enter. (Zastąp 136.142.35.137 adresem IP sieci ataku podanego przez instruktora). Jakie są wyniki skanowania SYN?

4. Następnie spróbuj wysłać nowy pakiet SYN na inny adres IP w zakresie ataku. Jakie są wyniki tego nowego skanowania? Czy widzisz jakieś różnice? Jeśli tak, wypisz je.

5. Nmap może skanować zakres adresów IP, więc nie jest konieczne wprowadzanie jednego adresu IP na raz. Aby wysłać pakiet SYN na każdy adres IP w zakresie ataku, wpisz nmap -sS -v 136.142.35.137-140 i naciśnij Enter. (Zastąp 136.142.35.137-140 zakresem adresów IP sieci atakującej podanym przez instruktora.)

6. Aby zobaczyć wynik w formacie przewijania, naciśnij klawisz strzałki w górę, dodaj opcję | less na końcu polecenia Nmap i naciśnij Enter. Polecenie powinno wyglądać następująco: nmap -sS -v 136.142.35.137-140 | less.

7. Następnie dodaj jeszcze jeden parametr do polecenia Nmap, aby określić, na których komputerach w zasięgu ataku uruchomiona jest usługa SMTP lub usługa HTTP. Korzystając z wiedzy zdobytej do tej pory w tej aktywności, wprowadź polecenie i zanotuj wynik. (Wskazówka: jakich portów używają SMTP i HTTP?) Wynik polecenia może się różnić, ale ważne jest nauczenie się, jak budować na poleceniu Nmap. Możesz wybrać określone porty w poleceniu Nmap, więc nie wszystkie 65 000 portów musi zostać przeskanowanych.

8. Pozostaw powłokę terminala otwartą na potrzeby następnej aktywności.

BAJTY BEZPIECZEŃSTWA

Pewnego wieczoru do pracy przyszedł specjalista ds. bezpieczeństwa i zauważył, że zapora sieciowa firmy uległa awarii, ponieważ ktoś uruchomił program skanujący porty w sieci, używając pakietów ACK. Wielu atakujących używa skanowania ACK, aby ominąć urządzenia filtrujące pakiety (takie jak zapory sieciowe). W tym przypadku zapora sieciowa firmy została wyłączona, ponieważ została zalana dziesiątkami tysięcy pakietów ACK bombardujących jej tabele routingu. To skanowanie ACK stanowiło atak DoS na sieć, więc nie bądź zbyt pewny siebie, uruchamiając skanowanie portów w sieciach. Zawsze uzyskaj pisemną zgodę właściciela sieci przed wykonaniem skanowania portów.

Aktywność 5-2: Korzystanie z dodatkowych poleceń Nmap

Czas trwania: 30 minut

Cel: Przeprowadzanie bardziej złożonych ataków skanowania portów za pomocą Nmap.

Opis: W tej aktywności nadal używasz Nmap do skanowania portów w swojej sieci atakującej. Dodajesz do parametrów używanych w Aktywności 5-1 za pomocą skryptów Nmap, aby odkryć więcej informacji o zdalnym hoście. Powinieneś ćwiczyć te polecenia, aż staną się drugą naturą, ale Fyodor opracował dobrze napisaną stronę pomocy (nazywaną „stroną podręcznika” w kręgach UNIX/Linux), której możesz użyć jako zasobu. Rozpoczynasz tę aktywność, przeglądając tę stronę pomocy.

1. Jeśli okno terminala nie jest otwarte, uruchom komputer w systemie Kali Linux, otwórz powłokę terminala i w wierszu poleceń wpisz man nmap i naciśnij Enter. Możesz zobaczyć, że to polecenie generuje więcej informacji niż polecenie nmap -h. Nie martw się o zapamiętywanie instrukcji; po prostu wiedz, że jest dostępna, gdy jej potrzebujesz.

2. Następnie wprowadź polecenie, aby wysłać domyślne skanowanie skryptu do 136.142.35.137 (nmap –sC –v 136.142.35.137). Możesz przeczytać więcej o domyślnych skryptach dołączonych do domyślnego ustawienia skanowania na stronie https://nmap.org/nsedoc/categories/default.html. Jakie są wyniki skanowania skryptu? Jaka marka i wersja serwera HTTP działa na portach 80 i 443?

3. Teraz ogranicz zakres, aby skanować tylko port 443, używając flagi –p (nmap –p44 3 –v 136.142.35.137). Dzięki temu skanowanie Nmap jest bardziej ukierunkowane i mniej zauważalne.

Nessus i OpenVAS (lub Greenbone Security Assistant)

Testerzy bezpieczeństwa powinni również zbadać Nessus. Nessus to narzędzie do oceny podatności od Tenable, które rozszerza możliwości NMAP poprzez analizę otwartych portów pod kątem określonych informacji o wersji i dostarcza szczegółowych informacji o podatnościach w odpowiedniej usłudze. Narzędzie do oceny podatności automatyzuje proces skanowania adresów IP, otwartych portów i podatności. Skanery podatności mają bazę danych znanych podatności i bazę danych wtyczek do sprawdzania bezpieczeństwa (skryptów i logiki), które są używane do sprawdzania podatności. Nessus Professional to produkt, który można kupić, ale Tenable oferuje bezpłatną wersję o nazwie Nessus

Essentials. Essentials ma takie same możliwości jak Nessus Professional, ale ogranicza liczbę adresów IP, które można przeskanować. Nessus Essentials jest przydatny do eksperymentów i nauki.

Nessus ma również rozwidlenie open-source o nazwie OpenVAS, obecnie markowane jako Greenbone Security Assistant. OpenVAS nie ma żadnych ograniczeń, więc możesz go używać jako narzędzia do oceny podatności, aby skanować dowolny adres IP. OpenVAS może aktualizować wtyczki sprawdzania bezpieczeństwa, gdy staną się dostępne. Wtyczka OpenVAS to program testowy bezpieczeństwa (skrypt), który można wybrać z interfejsu klienta. Osoba, która pisze wtyczkę, decyduje, czy oznaczyć ją jako niebezpieczną, a osąd autora na temat tego, co jest uważane za niebezpieczne, może różnić się od Twojego. Dlatego zaleca się pozostawienie włączonych bezpiecznych kontroli w polityce. Rysunek 5-4 przedstawia ekran główny interfejsu internetowego OpenVAS. Skanowanie OpenVAS nie ogranicza się do określania, które usługi są uruchomione na porcie. Wtyczki OpenVAS mogą również określać, jakie podatności są powiązane z tymi usługami.

PRZEPROWADZANIE PING SWEEPS

Skanery portów mogą być również używane do przeprowadzania ping sweep dużej sieci w celu zidentyfikowania, które adresy IP należą do aktywnych hostów. Innymi słowy, aby dowiedzieć się, które hosty są „aktywne", ping sweep po prostu pinguje zakres adresów IP i sprawdza, jaki typ odpowiedzi jest zwracany. Problem z poleganiem na ping sweep w celu zidentyfikowania aktywnych hostów polega na tym, że komputer może być wyłączony w momencie przeszukiwania i wskazywać, że adres IP nie należy do aktywnego hosta. Innym problemem z ping sweep jest to, że wielu administratorów sieci konfiguruje węzły tak, aby nie odpowiadały na żądanie echa ICMP (typ 8) odpowiedzią echa ICMP (typ 0). Ta odpowiedź nie oznacza, że komputer nie działa; oznacza to po prostu, że nie odpowiada komputerowi atakującemu. Dodaj możliwość filtrowania ruchu ICMP przez zaporę, a otrzymasz wiele powodów, aby zachować ostrożność podczas przeprowadzania ping sweep. Możesz użyć wielu narzędzi do przeprowadzenia skanowania ping sieci, a o niektórych z nich dowiesz się w poniższych sekcjach.

Fping

Za pomocą narzędzia Fping (www.fping.org) możesz pingować wiele adresów IP jednocześnie. Fping, dołączony do Kali Linux, może akceptować zakres adresów IP wprowadzonych w wierszu poleceń lub możesz utworzyć plik zawierający wiele adresów IP i użyć go jako danych wejściowych dla polecenia Fping. Na przykład polecenie fping -f ip_address.txt używa pliku ip_address.txt, który zawiera listę adresów IP, jako pliku wejściowego. Plik wejściowy jest zwykle tworzony za pomocą języka shellscripting, dzięki czemu nie musisz wpisywać tysięcy adresów IP potrzebnych do skanowania ping w sieci klasy B. Aby wykonać polecenie ping sweep zakresu adresów IP bez użycia pliku wejściowego, należy użyć polecenia fping -g BeginningIPAddress EndingIPAddress. Parametr -g jest używany, gdy nie jest dostępny żaden plik wejściowy.

Hping3

Możesz również użyć narzędzia Hping3 do wykonywania skanowań ping. Jednak wielu testerów bezpieczeństwa używa go do omijania urządzeń filtrujących poprzez wstrzykiwanie spreparowanych lub w inny sposób zmodyfikowanych pakietów IP. To narzędzie oferuje bogactwo funkcji, a testerzy bezpieczeństwa powinni poświęcić jak najwięcej czasu na naukę tego zaawansowanego narzędzia do skanowania portów. Aby uzyskać szybki przegląd, użyj polecenia hping3 -help | less i przejrzyj parametry, których możesz użyć . Jak widać, możesz dodać wiele parametrów do polecenia Hping3, co umożliwi Ci stworzenie pakietu IP na Twoje potrzeby. Podczas tworzenia pakietu IP w Ćwiczeniu 5-4 możesz odwołać się do tych rysunków podczas korzystania z narzędzia Hping3.

BAJTY BEZPIECZEŃSTWA

Jeśli zdecydujesz się na użycie ping sweeps, uważaj, aby nie uwzględnić adresu rozgłoszeniowego w zakresie adresów IP. Dołączenie go przez pomyłkę może się zdarzyć, jeśli w organizacji używane jest podsieciowanie. Na przykład, jeśli sieć IP 193.145.85.0 jest podzielona na podsieci 255.255.255.192, tworzone są cztery podsieci: 193.145.85.0, 193.145.85.64, 193.145.85.128 i 193.145.85.192. Adresy rozgłoszeniowe dla każdej podsieci to 193.145.85.63, 193.145.85.127, 193.145.85.191 i 193.145.85.255. Jeśli ping sweep zostanie przypadkowo aktywowany w zakresie hostów 193.145.85.65 do 193.145.85.127, nadmierna ilość ruchu może zalać sieć, ponieważ uwzględniony jest adres rozgłoszeniowy 193.145.85.127. Ten błąd jest większym problemem w przypadku adresu klasy B, ale jeśli wykonujesz ping sweep, upewnij się, że Twój klient podpisał pisemną umowę autoryzującą testowanie.

Tworzenie pakietów IP

Pakiety zawierają adresy IP źródłowe i docelowe, a także informacje o flagach, których nauczyłeś się wcześniej: SYN, ACK, FIN itd. Możesz utworzyć pakiet z określonym zestawem flag. Na przykład, jeśli nie jesteś zadowolony z odpowiedzi otrzymanej od komputera hosta po wysłaniu pakietu SYN, możesz utworzyć inny pakiet z ustawioną flagą FIN. Flaga SYN mogła zwrócić komunikat „zamknięty port", ale pakiet FIN wysłany do tego samego komputera może zwrócić komunikat „filtrowany port". Możesz tworzyć dowolny typ pakietu, jaki chcesz. Hping3 i Fping to pomocne narzędzia do tworzenia pakietów IP, a oba narzędzia wykorzystujesz w Aktywności 5-3.

Aktywność 5-3: Tworzenie pakietów IP za pomocą Fping i Hping3

Czas trwania: 30 minut

Cel: Naucz się tworzyć pakiety IP za pomocą Fping i Hping3.

Opis: W tej aktywności zobaczysz, jak testerzy bezpieczeństwa mogą tworzyć pakiety IP, aby dowiedzieć się, jakie usługi są uruchomione w sieci. Im więcej sposobów znasz, jak wysłać pakiet do nieświadomego portu na komputerze i uzyskać odpowiedź, tym lepiej. Jeśli komputer nie odpowiada na pakiet ICMP wysłany do określonego portu, nie oznacza to, że każdy pakiet wysłany do tego samego portu otrzyma tę samą odpowiedź. Być może będziesz musiał wysłać różne pakiety, aby uzyskać wyniki potrzebne do dokładnego testu bezpieczeństwa.

1. W razie potrzeby uruchom komputer w systemie Linux. Otwórz powłokę terminala, a następnie wpisz fping -h i naciśnij Enter.

2. Aby zobaczyć aktywne komputery w zakresie ataku podanym przez instruktora, wpisz fping -g BeginningIPaddress EndingIPaddress i naciśnij Enter. Zapisz wyniki. (Upewnij się, że używasz początkowego i końcowego adresu IP w zakresie ataku.)

3. Następnie wpisz hping3 -S IPAddressAttackedComputer (podmieniając adres IP z zakresu ataku) i naciśnij Enter. Używając parametru -S, tworzysz pakiet TCP SYN.

4. Otwórz inną powłokę terminala, a następnie wpisz tcpdump i naciśnij Enter.

5. Ustaw oba okna powłoki obok siebie, aby móc obserwować, co się stanie po wprowadzeniu polecenia Hping3. W powłoce, w której nie jest uruchomiony Tcpdump, naciśnij Ctrl+C, aby powrócić do wiersza poleceń, wpisz hping3 -S IPAddressAttackedComputer i naciśnij Enter. Obserwuj, jak okno Tcpdump wypełnia się generowanym ruchem. Aby zatrzymać Tcpdump przed przechwytywaniem pakietów, naciśnij Ctrl+C w tym oknie powłoki.

6. Jeśli masz czas, zapoznaj się ze stronami pomocy Hping3 i poeksperymentuj z tworzeniem różnych typów pakietów. Zwróć uwagę na różnice w ruchu sieciowym generowanym przez polecenie Tcpdump. Testerzy bezpieczeństwa muszą zrozumieć, w jaki sposób niewielkie zmiany w pakietach wysyłanych do zaatakowanego komputera mogą dawać różne rezultaty. Na przykład, jeśli komputer nie odpowiada na pakiet SYN, spróbuj wysłać pakiet ACK. Co się dzieje, gdy wysyłany jest pakiet FIN? Jeśli nie odnosisz żadnego sukcesu, spróbuj wysłać te same pakiety do różnych portów. Czy ta metoda zmienia odpowiedź zaatakowanego komputera?

7. Po zakończeniu zamknij obie powłoki.

ROZUMIENIE SKRYPTÓW

Niektóre narzędzia mogą wymagać modyfikacji, aby lepiej odpowiadały Twoim potrzebom jako testera bezpieczeństwa. Stworzenie dostosowanego skryptu — programu, który automatyzuje zadanie, którego ręczne wykonanie zajmuje zbyt dużo czasu — może być rozwiązaniem oszczędzającym czas. Jak wspomniano, Fping może używać pliku wejściowego do wykonywania skanowań ping. Jednak ręczne tworzenie pliku wejściowego z tysiącami adresów IP nie jest warte czasu. Zamiast tego większość testerów bezpieczeństwa polega na podstawowych umiejętnościach programistycznych, aby napisać skrypt do tworzenia pliku wejściowego.

Podstawy pisania skryptów

Jeśli pracowałeś z programowaniem wsadowym DOS, skrypty będą Ci znane. Jeśli jednak masz doświadczenie w sieciach i dopiero zaczynasz programować, zacznij od podstaw. Skrypt lub plik wsadowy to plik tekstowy zawierający wiele poleceń, które zwykle są wprowadzane ręcznie w wierszu poleceń. Jeśli używasz zestawu poleceń wielokrotnie, aby wykonać to samo zadanie, to zadanie może być dobrym kandydatem do skryptu. Możesz uruchomić skrypt, używając tylko jednego polecenia. Najlepszym sposobem nauki tworzenia scenariusza jest praktyka, dzięki czemu będziesz mieć okazję przećwiczyć pisanie scenariusza w Aktywności 5-4.

Aktywność 5-4: Tworzenie skryptu wykonywalnego

Czas trwania: 45 minut

Cel: Naucz się tworzyć, zapisywać i uruchamiać skrypt wykonywalny.

Opis: Wiele narzędzi hakerskich jest napisanych w językach skryptowych, takich jak VBScript lub JavaScript. W tej aktywności tworzysz skrypt, który wypełnia plik zakresem adresów IP. Ten typ pliku może być używany jako plik wejściowy dla Nmap lub Fping.

1. W razie potrzeby uruchom komputer w systemie Linux, a następnie otwórz powłokę terminala. Wpisz vim Myshell i naciśnij Enter.

2. Naciśnij i, aby przejść do trybu wstawiania. Jeśli po raz pierwszy używasz edytora vim, skorzystaj z Tabeli 5-1 jako odniesienia. Nazwa „vim” oznacza „vImproved”, ponieważ opiera się na funkcjonalności starszego edytora tekstu vi. Jeśli w przeszłości miałeś problemy z vi, vim jest łatwiejszy w użyciu. (Aby uzyskać bardziej szczegółowy opis tego wszechstronnego edytora, wpisz man vim w innej powłoce terminala i naciśnij Enter.)

3. Wpisz #!/bin/sh i naciśnij Enter. Ten wiersz identyfikuje plik, który piszesz jako skrypt. Powinieneś wprowadzić kilka wierszy dokumentacji do wszystkich skryptów lub programów, które piszesz, ponieważ pomagają one później w modyfikacjach i konserwacji programu. Gdy wiersz jest używany do celów dokumentacji, jest poprzedzony znakiem #.

4. Drugi wiersz to nazwa tworzonego skryptu. Wpisz # Myshell i naciśnij Enter. Gdyby ten skrypt był używany w środowisku produkcyjnym, wprowadziłbyś również datę i swoje imię.

5. Przeczytaj komentarze do dokumentacji dotyczące celu skryptu, ale nie wpisuj ich w swoim skrypcie. Twój skrypt powinien zawierać tylko polecenia #!/bin/sh i # Myshell.

6. Wpisz network_id=”193.145.85.” i naciśnij Enter. Pamiętaj o dodaniu cudzysłowów i kropki po 85. (Ponieważ nie używasz tego skryptu w aktywnej sieci, adres wprowadzony w tym wierszu nie ma znaczenia.)

7. Wpisz count=0 i naciśnij Enter. To polecenie inicjuje zmienną count do zera, co jest zawsze mądre, ponieważ zmienna nie powinna być używana w programie bez ustawienia wartości. Twój skrypt musi dodać liczbę 1 do identyfikatora sieci 193.145.85. i kontynuować zwiększanie i dodawanie liczb do identyfikatora sieci, aż zakres adresów IP od 193.145.85.1 do 193.145.85.254 zostanie zapisany w pliku o nazwie ip_address.txt. W programowaniu ten powtarzający się proces nazywa się pętlą. Aby uniknąć tworzenia pętli nieskończonej, musisz dodać warunek w instrukcji while.

8. Wpisz while [“$count” -le 253] i naciśnij Enter. Zwróć uwagę na spacje w nawiasach kwadratowych i zwróć szczególną uwagę na użycie cudzysłowów i znaków dolara.

9. Wpisz do i naciśnij Enter. W tym poleceniu skrypt wykonuje swoje główne zadanie. Akcja ma miejsce pomiędzy poleceniem do a poleceniem done (dodanym w kroku 11). Aby zwiększyć zmienną count o 1, wpisz count=$(($count+1)), zwracając szczególną uwagę na nawiasy, i naciśnij Enter.

10. Wpisz printf “%s%s\n” $network_id $count >> ip_address.txt i naciśnij Enter. To polecenie używa funkcji printf do zapisu danych do pliku. Znaki >> dodają każdy adres IP na końcu pliku ip_address.txt.

11. Wpisz done i naciśnij Enter, a następnie wpisz exit 0 i naciśnij Enter. Rysunek 5-11 przedstawia cały skrypt. Zapisz swoją ciężką pracę, naciskając Esc i wpisując : (dwukropek). W wierszu poleceń : wpisz wq i naciśnij Enter.

12. Teraz, gdy zapisałeś skrypt, musisz uczynić go wykonywalnym, aby móc go uruchomić. W wierszu poleceń wpisz chmod +x Myshell i naciśnij Enter.

13. Aby uruchomić skrypt, wpisz ./Myshell i naciśnij Enter. Ponieważ skrypt nie tworzy żadnego wyjścia na ekranie, musisz sprawdzić zawartość pliku ip_address.txt, aby sprawdzić, czy skrypt zadziałał.

14. Wpisz cat ip_address.txt i naciśnij Enter. Ile adresów IP zostało utworzonych w pliku ip_address.txt?

15. Zamknij powłokę. Możesz pozostawić system uruchomiony na potrzeby projektów kończących moduł.

PODSUMOWANIE MODUŁU

• Skanowanie portów, zwane również skanowaniem usług, to proces badania zakresu adresów IP w celu ustalenia, jakie usługi są uruchomione w systemie lub sieci.

• Różne skany portów mogą wywoływać różne informacje, dlatego testerzy bezpieczeństwa muszą być świadomi typów skanowania portów, takich jak SYN, ACK, FIN itd.

• Dostępnych jest wiele narzędzi do skanowania portów. Najpopularniejsze to Nmap, Nessus i OpenVAS.

• Przeszukiwania pingów służą do określania, które komputery w sieci są „aktywne” (komputery, do których może dotrzeć komputer atakujący).

• Korzystanie ze skryptów może pomóc specjalistom ds. bezpieczeństwa poprzez automatyzację czasochłonnych zadań.