Skanowanie i enumeracja w ramach etycznego hakowania

Po fazie odcisku palca zgromadzisz wystarczająco dużo ogólnych informacji o celu, aby rozpocząć głębszą analizę i uzyskać bardziej szczegółowe informacje o znalezisku. Ten kolejny etap, zwany fazą skanowania i enumeracji, przetwarza część wcześniej pozyskanych informacji. Uzyskujemy tu informacje o dostępnych portach, uruchomionych usługach i sieci. W tym rozdziale określimy, które systemy znajdują się w sieci (znane również jako systemy aktywne) i są osiągalne. Przyjrzymy się również systemom nasłuchującym połączeń i omówimy enumerację, wykorzystując różnorodne narzędzia i techniki.

Porównanie skanowania i enumeracji

Zanim zagłębimy się w techniki skanowania i enumeracji, musimy omówić różnice między nimi. Wielu specjalistów ds. bezpieczeństwa używa terminów „skanowanie" lub „skanowanie" jako ogólnych określeń dla całego procesu skanowania i enumeracji. Chociaż można je luźno stosować zamiennie, w rzeczywistości nie są to te same pojęcia. Zdefiniujmy te terminy, aby to wyjaśnić:

• Skanowanie to czynność przeszukiwania czegoś w celu uzyskania od niego informacji. Na przykład, skanujemy port, aby sprawdzić, jaka usługa jest uruchomiona, i skanujemy komputer, aby sprawdzić, czy odpowiada.

• Enumeracja to iteracja list, obliczonych lub zebranych. Może to być lista portów, komputerów itd.

Należy pamiętać, że skanowanie i enumeracja nie ograniczają się tylko do obwodu sieci. Ten etap może i jest często powtarzany w miarę pojawiania się nowych informacji. Przykładem jest sytuacja, gdy atakujący przeskanuje i skutecznie spenetruje obwód sieci. Atakujący ma teraz dostęp do sieci wewnętrznej, którą należy przeskanować i zrozumieć. W obu przypadkach, zarówno zewnętrznie, jak i wewnętrznie, celem skanowania sieci jest:

• Identyfikacja hostów w sieci

• Identyfikacja otwartych i zamkniętych portów na każdym hoście

• Identyfikacja miejsca, w którym znajduje się system operacyjny – czyli Windows, Linux lub Mac

• Identyfikacja usług działających w sieci

• Identyfikacja procesów działających w sieci

• Identyfikacja obecności systemów bezpieczeństwa, takich jak zapory sieciowe i programy antywirusowe

• Identyfikacja architektury systemu i sieci

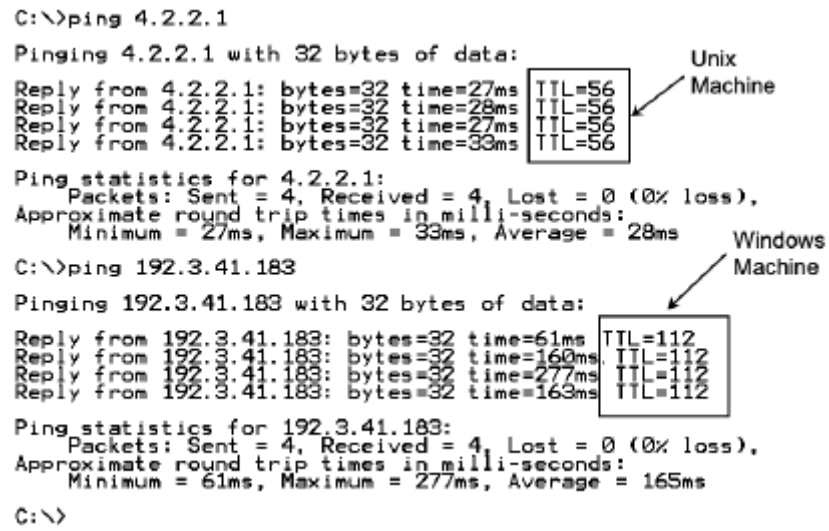
• Identyfikacja luk w zabezpieczeniach

Mając to na uwadze, specjaliści ds. bezpieczeństwa często mają na myśli enumerację listy hostów, portów, adresów IP itd., skanując każdy z nich w poszukiwaniu danych. Przyjrzyjmy się teraz typom skanowań, które możemy przeprowadzić, i temu, jak możemy dodać do nich enumerację.

Ping

Inżynierowie sieciowi dawno temu dowiedzieli się, że potrzebują sposobu na sprawdzenie, czy systemy zdalne są online. Stworzyli protokół ICMP (Internet Control Message Protocol) jako narzędzie wspomagające rozwiązywanie problemów sieciowych. Podstawą protokołu ICMP jest narzędzie o nazwie Ping. Ping oferuje kilka funkcji; jednak najważniejsze, z którymi większość osób jest

zaznajomiona, to ICMP_ECHO_REQUEST, znany również jako typ 8, oraz ICMP_ECHO_REPLY, znany również jako typ 0. Ping to bardzo proste narzędzie, które można uruchomić za pomocą polecenia ping, po którym następuje adres IP lub nazwa domeny. Przykładem może być polecenie ping 192.168.100.54 lub pingowanie nazwy domeny, takiej jak ping cnn.com. To polecenie nakazuje maszynie wysłanie żądania echa ICMP (typ 8). Miejmy nadzieję, że system po drugiej stronie połączenia jest dostępny i może odpowiedzieć, czyli odpowiedzieć echem ICMP (typ 0). Narzędzie ping jest bardzo przydatne i dostarcza wielu informacji wykraczających poza samo informowanie o obecności i odpowiedzi komputera. Po pierwsze, podaje czas reakcji, pozwalający zdiagnozować ewentualne problemy z komunikacją w sieci. Inną interesującą cechą polecenia ping jest ostatni element, tzw. czas życia (TTL), który jest miarą liczby przeskoków lub routerów, jakie komputer musi pokonać, aby dotrzeć do systemu na drugim końcu. Za każdym razem, gdy żądanie ping przechodzi przez router, wartość TTL jest zmniejszana o jeden. Warto zauważyć, że systemy Microsoft i Unix implementują to inaczej, używając różnych wartości początkowych. Komputery Unix rozpoczynają od wartości TTL równej 64, a komputery Microsoft Windows od wartości TTL równej 128. Poniższy rysunek przedstawia przykłady żądania ping i odpowiedzi z różnymi wartościami TTL:



Korzystając z poprzedniego przykładu, można ustalić, że adres IP 4.2.2.1 jest maszyną Unix i jest oddalony o około osiem przeskoków, czyli routerów. Ponadto adres IP 192.3.41.183 jest maszyną Microsoft Windows i jest oddalony o około 16 przeskoków, czyli routerów. Kluczowym wnioskiem jest to, że dzięki wbudowanemu narzędziu nie tylko byliśmy w stanie określić, czy system odpowiada, ale także byliśmy w stanie odcisk palca systemu operacyjnego po drugiej stronie. Teraz zła wiadomość — jest to dobrze znana technika odcisku palca systemu. W odpowiedzi obrońcy wdrażali metody zapobiegania temu z zewnątrz sieci, co nieco ograniczyło użyteczność polecenia ping w rekonesansie. Nie oznacza to jednak, że wszystkie zabezpieczenia zostały zaktualizowane i że nie należy go próbować. Ponadto polecenie ping rzadko jest blokowane po ustanowieniu przyczółka w sieci i działaniu wewnątrz. Z tego powodu możliwe jest wykonanie polecenia ping na dużą skalę; znane jest to również jako ping sweep. Przyjrzyjmy się temu.

Pingowanie na dużą skalę

Pingowanie działa świetnie w kilku systemach, ale jak można go używać w dużej sieci? Pingowanie każdego możliwego adresu hosta poprzez indywidualne uruchamianie polecenia ping jest czasochłonne. Użycie aplikacji lub skryptu do uruchomienia polecenia ping na dużą skalę jest często określane jako ping sweep. Ta technika służy do identyfikacji systemów dostępnych i niedostępnych na dużą skalę. Ping sweep został pierwotnie opracowany poprzez powiązanie polecenia ping z listą

adresów; później aplikacje takie jak Nmap zostały opracowane w celu zautomatyzowania tego procesu. Ping sweep, jak sama nazwa wskazuje, pinguje grupę urządzeń i pomaga atakującemu określić, które z nich są aktywne. Ping sweep pomaga w mapowaniu sieci poprzez odpytywanie bloków sieci lub list adresów IP lub domen. Jak więc skalować ping, aby wykonać skanowanie? Można napisać własny skrypt lub narzędzie, które pobiera listę pingów do każdego systemu na liście. Alternatywnie, można skorzystać z jednego z wielu dostępnych narzędzi. Kilku dostawców oferuje narzędzia do pingowania, które oferują różne poziomy funkcjonalności i dodatkowe funkcje, takie jak możliwość pingowania. Oto kilka z nich:

• Solarwinds (komercyjny): Oferuje monitorowanie sieci i skanowanie pingiem w celu określenia, czy systemy działają, czy nie.

• Advanced IP Scanner (bezpłatny): Narzędzie graficzne z interfejsem użytkownika systemu Windows, zaprojektowane do łatwego skanowania sieci.

• Fping (bezpłatny): Narzędzie wiersza poleceń dla systemu Linux do przeprowadzania skanowania pingiem na dużą skalę.

• Angry IP Scanner (bezpłatny): Narzędzie graficzne z interfejsem użytkownika systemu Windows do szybkiego skanowania pingiem i portów.

• Nmap/Zenmap (bezpłatny): Narzędzie dla systemów Linux/Windows do przeprowadzania skanowania pingiem, portów itp.

To tylko kilka z dostępnych narzędzi do wykonywania skanowań ping i nie tylko. Skupimy się przede wszystkim na narzędziu do skanowania sieci Nmap, które jest częścią instalacji Kali Linux, i pokażemy, jak z niego korzystać w sekcji „Wprowadzenie do narzędzia do skanowania sieci Nmap". Najpierw przyjrzyjmy się innemu wbudowanemu narzędziu, Traceroute, i zobaczmy, jak możemy go wykorzystać w procesie skanowania sieci.

Traceroute

Traceroute, lub Tracert w przypadku komputera z systemem Windows, to narzędzie służące do mapowania routerów między użytkownikiem a hostem docelowym. Robi to poprzez tworzenie specjalnie spreparowanych pakietów ping, w których wartość TTL jest zwiększana o jeden, aż do momentu dotarcia do hosta docelowego. Jak wspomniano wcześniej, dla każdego routera, przez który przechodzi pakiet ping, wartość TTL jest zmniejszana o jeden. Jeśli wartość TTL spadnie do zera, do hosta, który zainicjował pakiet, wysyłany jest komunikat o błędzie. Następnie narzędzie dodaje kolejny jeden do wartości TTL, aż do zakończenia procesu. Za każdym razem, gdy pakiet przechodzi przez router, informacja jest wyświetlana na ekranie:

```
┌──(kali㉿kali)-[~]
└─$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  SL-WF2G (192.168.100.1)  3.369 ms  3.215 ms  3.105 ms
 2  192.168.10.1 (192.168.10.1)  4.232 ms  4.183 ms  4.136 ms
 3  * * *
 4  te0-6-2-0---0.lcr01.clwr.fl.frontiernet.net (172.99.44.98)  9.965 ms
(172.99.45.88)  9.874 ms
 5  ae8---0.scr02.mias.fl.frontiernet.net (74.40.3.73)  16.358 ms  16.312
 6  ae0---0.cbr03.mias.fl.frontiernet.net (45.52.201.145)  23.542 ms ae1-
ernet.net (45.52.201.147)  17.150 ms  17.076 ms
 7  static-74-43-96-158.fnd.frontiernet.net (74.43.96.158)  14.355 ms  13
 8  * * *
 9  dns.google (8.8.8.8)  14.156 ms  13.585 ms  13.517 ms
```

Na powyższym zrzucie ekranu widzimy przykładowy kod śledzenia trasy do serwera DNS Google pod adresem 8.8.8.8. Pakiet opuszcza sieć wewnętrzną pod adresem 192.168.100.1 i przechodzi przez siedem routerów, zanim dotrze do systemu docelowego. Należy zauważyć, że dwa routery mają znaki * * * zamiast nazw lub adresów IP. Zazwyczaj oznacza to, że routery te zostały skonfigurowane tak, aby nie zwracały informacji do narzędzia traceroute.

Ważna uwaga

W innych przypadkach, nie tylko podczas skanowania ping, ale także podczas innych typów skanowania, zapory sieciowe i inne urządzenia zabezpieczające mogą po prostu odrzucać żądania w ramach ochrony innych urządzeń sieciowych. Jeśli używasz narzędzi takich jak Nmap, mogą one nie zgłaszać blokady, a jedynie oznaczać ją jako niedostępną. Jednym z niewielu sposobów, aby mieć pewność, że pingi/skanowania dotrą do celu, jest użycie aplikacji do przechwytywania pakietów, takiej jak Wireshark, w celu przechwytywania i inspekcji ruchu sieciowego na poziomie pakietów.

Teraz możesz się zastanawiać, jak to narzędzie jest przydatne dla atakującego; w rzeczywistości jest ono przydatne na dwa sposoby:

• Podczas mapowania obwodu, ostatnie routery w widoku traceroute będą częścią sieci docelowej. Innymi słowy, możemy być w stanie zmapować urządzenia, takie jak router zewnętrzny i zaporę sieciową, między obwodem a urządzeniem docelowym.

• Gdy atakujący uzyska dostęp do sieci, zwłaszcza dużej, może użyć tego narzędzia do zmapowania infrastruktury routerów w ramach ataku.

Podsumowując, zarówno ping, jak i traceroute to niezwykle przydatne narzędzia zarówno dla atakujących, jak i broniących się przed nimi hakerów etycznych. Po pierwsze, narzędzie to jest dostępne na każdym komputerze, co oznacza, że nie trzeba go pobierać ani instalować. Po drugie, narzędzia te są wykorzystywane przez administratorów i techników do rozwiązywania problemów z siecią, zgodnie z ich przeznaczeniem. Jeśli sieć nie jest zablokowana wewnętrznie, prawdopodobnie nie będzie monitorowana w znaczący sposób. Z odrobiną czasu i cierpliwości atakujący może zmapować całą sieć za pomocą łatwo dostępnych narzędzi, nie informując nikogo o swojej obecności. Skoro omówiliśmy już identyfikację hostów online i enumerację zarówno hostów, jak i routerów, przyjrzyjmy się identyfikacji otwartych portów i usług.

Zrozumienie enumeracji usług

Po ustaleniu, które systemy są dostępne i odpowiadają, następnym krokiem jest sprawdzenie, jakie usługi są dostępne. Usługi takie jak serwery poczty e-mail i WWW otwierają porty do komunikacji.

Najprostszym sposobem ich znalezienia jest przeprowadzenie skanowania portów. Zanim przejdziemy do omówienia skanowania portów, ważne jest zrozumienie portów i ich działania.

Wprowadzenie do portów

W każdym systemie dostępnych jest łącznie 65 535 portów TCP i 65 535 portów UDP. Mogłoby się wydawać, że trzeba zapamiętać wszystkie porty; jednak pierwsze 1024 z tych portów, znane również jako porty dobrze znane, są powszechnie kojarzone z określonymi usługami. Przykładem są serwery WWW, które zazwyczaj działają na porcie 80 w systemie. Listę tych przypisań portów można łatwo znaleźć, szybko przeszukując internet; jednak oficjalną listę prowadzi organizacja Internet Assigned Numbers Authority (IANA), którą można znaleźć pod adresem https://www.iana.org/. Warto również zauważyć, że lista ta stanowi raczej wskazówkę niż regułę. Inżynierowie mogą konfigurować usługi tak, aby korzystały z różnych portów z dowolnego powodu. Każdy zidentyfikowany port będzie powiązany z określonym procesem na komputerze, który w dowolnym momencie wysyła lub odbiera informacje. Jeśli skanowanie portów zwróci porty, których nie można od razu rozpoznać, należy dokładniej przeanalizować ich numery, aby określić ich naturę. Teraz, gdy znamy już podstawowe informacje na temat portów, przyjrzyjmy się, jak działa skanowanie portów.

Jak działa skanowanie portów?

Skanowanie portów ma na celu sprawdzenie portu w celu ustalenia, czy odpowiada i jest dostępny do komunikacji w sieci. Przyjrzyjmy się trzem komponentom:

1. W normalnej komunikacji z usługą komputer inicjuje komunikację za pośrednictwem protokołu TCP. Protokół TCP używa flag, czyli kombinacji flag, do sterowania komunikacją. Aby nawiązać komunikację, używa specjalnego zestawu flag, znanego jako potrójne uzgadnianie. Potrójne uzgadnianie to seria pakietów (dokładnie trzech), które nawiązują komunikację. Pierwszy pakiet, pochodzący od komputera żądającego, to pakiet synchronizacji (SYN). Można to porównać do sytuacji, gdy ktoś podnosi słuchawkę i wybiera numer; dzwonienie to próba rozmowy z kimś lub synchronizacji.

2. Kolejnym etapem łańcucha komunikacji jest synchronizacja i potwierdzenie (SYN-ACK). Zgodnie z analogią do telefonu, miałoby to miejsce, gdy osoba po drugiej stronie odbiera telefon i mówi „dzień dobry".

3. Ostatnim pakietem w potrójnym uzgadnianiu jest ACK. Ta ostatnia część jest równoważna z odpowiedzią dzwoniącego na komunikat powitalny i rozpoczęciem rozmowy.

W ten sposób działa potrójne uzgadnianie TCP i służy do nawiązania niezawodnej komunikacji. Dodatkowo, po nawiązaniu komunikacji, do sterowania komunikacją używane są następujące flagi:

• Reset (RST): Oznacza to, że port nie akceptuje żądań.

• Finish (FIN): Oznacza to, że rozmowa jest zakończona, a sesja zostaje przerwana. Zarówno nadawca, jak i odbiorca wyślą pakiety FIN, aby płynnie zakończyć połączenie.

• Push (PSH): Oznacza to, że wysłane dane trafiają bezpośrednio do aplikacji, zamiast być buforowane.

• Urgent (URG): Oznacza to, że wysłane dane zostaną przetworzone natychmiast.

Skoro już wiesz o flagach komunikacyjnych, możesz zrozumieć, że pentesterzy, atakujący i inni mogą manipulować procesem komunikacji i flagami, tworząc pakiety TCP, mające na celu uzyskanie

informacji o uruchomionych aplikacjach lub usługach. Jak wspomniano, jednym z mechanizmów skanowania portów jest użycie flag. Typowe lub popularne metody skanowania portów TCP obejmują:

• Skanowanie połączenia TCP: Ten typ skanowania jest niezawodny, ponieważ wymaga ukończenia uzgadniania TCP; jednak jest również najłatwiejszy do wykrycia. Jeśli port jest otwarty i dostępny, odpowiedź to SYN/ACK; jeśli port jest zamknięty lub nie odpowiada, odpowiedź to RST/ACK.

• Skanowanie TCP SYN: Ten typ skanowania jest również znany jako skanowanie półotwarte, ponieważ uzgadnianie TCP nie jest ukończone. Niekompletne uzgadnianie nadal dostarcza atakującym wystarczającej ilości danych, aby mogli sprawdzić, czy system działa, jednocześnie próbując działać w ukryciu i ominąć systemy bezpieczeństwa.

• Skanowanie TCP FIN: Ten typ skanowania próbuje wykryć port, wysyłając żądanie zamknięcia nieistniejącego połączenia. Ten typ ataku polega na wysłaniu pakietu FIN do portu docelowego; jeśli port odpowie RST, sygnalizuje zamknięcie portu. Ta technika jest zazwyczaj skuteczna tylko na urządzeniach Unix.

• Skanowanie TCP NULL: W tym skanowaniu tworzone są specjalnie zaprojektowane pakiety, w których flagi TCP nie są ustawione. Ponieważ narusza to zasady komunikacji TCP, jest to próba uzyskania odpowiedzi od systemu i ewentualnego ujawnienia, czy port jest rzeczywiście otwarty, czy zamknięty.

• Skanowanie TCP ACK: To skanowanie wysyła spreparowany pakiet z ustawioną flagą ACK, aby wywołać odpowiedź listy kontroli dostępu (ACL) i poinformować atakującego, że port jest dostępny, ale lista ACL jest aktywna.

• Skanowanie TCP Xmas Tree: To skanowanie działa poprzez wysyłanie pakietów do portu docelowego z ustawionymi flagami w kombinacjach, które są niedozwolone lub nielogiczne (na przykład FIN, PSH i URG). Wyniki są następnie monitorowane w celu sprawdzenia reakcji systemu. Zamknięte porty powinny zwrócić RST.

Protokół TCP oferuje ogromne możliwości i elastyczność, które mogą zostać wykorzystane na korzyść atakującego. Niestety, protokół UDP, często używany do strumieniowego przesyłania danych, takich jak treści wideo i muzyka, nie oferuje takich możliwości. Wynika to głównie ze sposobu, w jaki protokół ten został zaprojektowany i do czego jest wykorzystywany. UDP, czasami nazywany protokołem zawodnym, można postrzegać jako komunikację typu best-effort i jako taki nie wykorzystuje żadnych flag ani nie oferuje żadnej informacji zwrotnej, jaką zapewnia TCP, co znacznie utrudnia manipulację i skanowanie portów. Na tym etapie atak przyjął bardziej interaktywne i agresywne podejście. Dostępnych jest wiele narzędzi do mapowania otwartych portów i identyfikacji usług działających na serwerach w sieci docelowej.

Problemy ze skanowaniem portów

Podczas skanowania sieci należy podjąć pewne środki ostrożności; dotyczy to zarówno atakujących, jak i obrońców:

• Po pierwsze, nie należy wyłączać sieci i jej psuć, ponieważ bezużyteczna sieć jest bezużyteczna.

• Kolejną rzeczą, którą powinni rozważyć obrońcy, jest unikanie tworzenia dodatkowych problemów poprzez generowanie alertów i zgłoszeń w celu ich rozwiązania. Należy poświęcić trochę czasu na zaplanowanie podejścia do skanowania portów lub mapowania sieci i zastosować odpowiednie mechanizmy kompensacyjne, informując wszystkie zaangażowane strony o istocie planu i jego celu.

• Należy również zwrócić uwagę na następujące kwestie:

- Fałszywe alarmy: Niektóre programy używają numerów portów zarejestrowanych w innych programach, co może powodować fałszywe alarmy podczas skanowania portów. Może to prowadzić do tworzenia niepotrzebnych bloków legalnych programów. Gdy pojawi się interesujący element, należy poświęcić trochę czasu na jego dokładniejsze zbadanie przed zastosowaniem mechanizmów kontroli i blokad.

- Fałszywe alarmy: Skanowanie portów może być intensywne dla komputera wykonującego daną operację. Czasami może to wyczerpać zasoby, generując fałszywe alarmy, ponieważ komputer nie jest już w stanie prawidłowo przetwarzać zwracanych danych. - Duży ruch: Skanowanie portów, zwłaszcza skanowanie portów, może generować duże obciążenie sieci, wprowadzając opóźnienia. Mając to na uwadze, zazwyczaj zaleca się przeprowadzanie skanowania poza normalnymi godzinami pracy, jeśli ma to być skanowanie rozległe i obejmujące cały system.

- Awaria systemu: Wiadomo, że skanowanie może powodować awarie systemów, zwłaszcza w przypadku prób skanowania w poszukiwaniu luk w zabezpieczeniach, które mogą uniemożliwić działanie systemu. Jak wspomniano wcześniej, należy starannie zaplanować skanowanie i zakres wykonywanych czynności oraz powiadomić o tym odpowiednie osoby.

- Niezarejestrowane numery portów: Wiele używanych numerów portów nie jest zarejestrowanych, co utrudnia identyfikację oprogramowania, które z nich korzysta.

Chociaż skanowanie portów jest skutecznym narzędziem dla etycznych hakerów lub atakujących, istnieją pewne mechanizmy obronne, które można wykorzystać, aby uniemożliwić skanowanie, utrudnić je lub zmniejszyć jego niezawodność. Omówmy niektóre z nich.

Środki zaradcze podczas skanowania

Istnieje więcej technik, niż można tu omówić; jednak poniższa lista zawiera kilka technik, które można zastosować, aby uniemożliwić atakującemu uzyskanie informacji ze skanowania portów, zaczynając od zapory sieciowej:

• Reguła „odmów wszystko”: Ta podstawowa reguła zapory sieciowej blokuje cały ruch do wszystkich portów, chyba że został on wyraźnie zatwierdzony.

• System wykrywania włamań (IDS): Wprowadź system IDS za zaporą sieciową, który analizuje ruch w celu identyfikacji skanowań.

• Testowanie zapory sieciowej: Przetestuj i zweryfikuj możliwości zapory sieciowej oraz jej reguły wykrywania i blokowania niepożądanego ruchu.

• Test skanowania portów: Użyj tych samych narzędzi, co atakujący, do skanowania i testowania, aby lepiej zrozumieć, jak wygląda skanowanie oraz co wykrywają i ostrzegają o nim mechanizmy kontroli.

Po przekroczeniu granicy sieci wielu atakujących uważa, że sieć wewnętrzna jest słaba i mniej bezpieczna. Zazwyczaj wynika to z faktu, że ze względów biznesowych kontrole bezpieczeństwa są łagodzone, co pozwala firmie działać bez przeszkód. Istnieje kilka technik, które można zastosować w sieci wewnętrznej, a które mogą okazać się pomocne. Oto niektóre z nich:

• Segmentacja sieci: Podzielenie sieci na logiczne segmenty utrudnia szerokie skanowanie.

• Listy kontroli dostępu (ACL) na routerach wewnętrznych: Listy kontroli dostępu (ACL) mogą być używane do blokowania lub odrzucania ruchu w oparciu o reguły bardzo podobne do tych, które są implementowane na zaporze sieciowej.

• Wdrożenie systemu SIEM lub systemu alarmowego: System SIEM (Security Information and Event Management) umożliwia wykrywanie zachowań sieciowych, takich jak skanowanie.

• Przeprowadzanie wewnętrznych skanowań w systemach dedykowanych: Podczas korzystania z aplikacji używanych przez atakujących, takich jak Nmap, mogą wystąpić fałszywe alarmy. Aby uniknąć nieporozumień, należy wykonywać te operacje w systemach dedykowanych, które można szybko zidentyfikować, i rozważyć wdrożenie reguł lub wyjątków dla tych systemów, aby zapobiec niepotrzebnym alertom.

• Systemy ochrony punktów końcowych: W ostatnich latach pojawiło się oprogramowanie do monitorowania punktów końcowych, które pozwala personelowi ochrony nie tylko monitorować sieć, ale także oceniać i ostrzegać o konkretnym komputerze. Oprogramowanie to posiada reguły wykrywające typowe wektory ataków, takie jak skanowanie portów, i nie tylko je blokuje, ale także powiadamia personel, aby uświadomić mu takie zachowanie.

Choć nie są w stanie tego konkretnie powstrzymać, można zarządzać alertami, aby wykryć to na wczesnym etapie. To tylko niektóre ze środków zaradczych i technik, które można wdrożyć, aby ograniczyć ryzyko skanowania. Ponieważ nie możemy tu omówić wszystkich narzędzi, konieczne jest ograniczenie dyskusji do tych, które są powszechnie używane i dobrze znane. Skupimy się na Nmap; jednak każde narzędzie oferujące tę samą funkcjonalność, w tym skanowanie i enumerację, będzie tutaj odpowiednie. Przyjrzyjmy się teraz narzędziu skanującemu Nmap.

Przedstawiamy narzędzie do skanowania sieci Nmap

Narzędzie Nmap to powszechnie używane narzędzie przez większość testerów penetracyjnych i hakerów etycznych. Jest ono stale aktualizowane przez aktywną grupę współpracowników tego projektu open source. Nmap to przede wszystkim skaner portów, pokazujący, które porty TCP i UDP są otwarte w systemie docelowym. Jednak Nmap to nie tylko skaner portów. Oferuje również wiele innych funkcji, w tym skanowanie pingów, odcisk palca systemu operacyjnego i śledzenie tras. Można go nawet rozszerzyć o silnik skryptowy Nmap (NSE), stając się uniwersalnym skanerem luk w zabezpieczeniach. Przyjrzymy się każdej z tych funkcji. Podczas korzystania z Nmapa pomocne może być wyświetlanie przez samo narzędzie podsumowania wysyłanych pakietów. Przełącznik polecenia do wywołania tego to –packet-trace. Wyświetla różne komunikaty o stanie na wyjściu, w tym niektóre wywołania funkcji connect() wysyłane lub odbierane, używany protokół (TCP lub UDP) oraz źródłowe i docelowe adresy IP i porty. Wyświetla również inne informacje nagłówkowe, takie jak TTL IP i numer sekwencyjny TCP. Polecenie Nmap do śledzenia pakietów wyglądałoby następująco:

Sudo nmap -Pn -sS 4.2.2.1 -p 1-1024 –packet-trace

Przyjrzyjmy się bliżej temu poleceniu, aby lepiej je zrozumieć:

• Parametr -Pn oznacza, że nie chcemy pingować systemu docelowego, tylko go przeskanować.

• Parametr -sS oznacza, że chcemy przeprowadzić skanowanie SYN.

• Parametr -p 1-1024 nakazuje programowi Nmap skanowanie tylko portów od 1 do 1024.

• Opcja –packet-trace powoduje, że program Nmap wyświetla status i podsumowanie pakietów.

Zrzut ekranu, dla porównania, wygląda następująco:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sS 4.2.2.1 -p1-1024 -packet-trace
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 23:24 EST
NSOCK INFO [0.0280s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0280s] nsock_connect_udp(): UDP connection requested to 192.168.255.3:53 (IOD #1
SENT (13.0981s) TCP 192.168.255.110:38202 > 4.2.2.1:23 S ttl=59 id=55880 iplen=44  seq=3467997
SENT (13.0983s) TCP 192.168.255.110:38202 > 4.2.2.1:25 S ttl=52 id=44523 iplen=44  seq=3467997
SENT (13.0984s) TCP 192.168.255.110:38202 > 4.2.2.1:587 S ttl=54 id=42861 iplen=44  seq=346799
SENT (13.0984s) TCP 192.168.255.110:38202 > 4.2.2.1:139 S ttl=47 id=25703 iplen=44  seq=346799
```

Jeśli użytkownik zapomni uruchomić Nmapa z opcją –packet-trace, może ją włączyć po uruchomieniu Nmapa, naciskając klawisz P. Jeśli nie chce już widzieć śladu pakietów, może użyć kombinacji klawiszy Shift + P, aby wyłączyć śledzenie pakietów. Dodatkowo, podczas skanowania, naciśnięcie dowolnego klawisza spowoduje wyświetlenie na ekranie bieżącego stanu, pokazującego czas, który upłynął, liczbę ukończonych hostów, liczbę aktywnych i aktywnych hostów oraz liczbę hostów aktualnie skanowanych równolegle. Inne klawisze, których można używać podczas skanowania, to klawisz V do zwiększania szczegółowości oraz klawisz D do włączania trybów debugowania. Inną funkcją obsługiwaną przez Nmapa jest sterowanie skanowaniem, w tym losowością i szybkością. Przyjrzymy się temu w następnej sekcji.

Sterowanie szybkością skanowania Nmap

Szybkość skanowania można kontrolować z poziomu wiersza poleceń, dodając parametr -T, a następnie liczbę od 0 do 5. Wraz ze wzrostem tych liczb rośnie również szybkość skanowania, co odpowiada następującym trybom:

• T0 (tryb paranoiczny): Ten tryb został zaprojektowany do powolnego skanowania, aby uniknąć typowych reguł wykrywania stosowanych przez systemy IDS i SIEM. Nmap robi to, wysyłając pakiety co około pięć minut. Dodatkowo, w trybie paranoicznym żadne pakiety nie są wysyłane równolegle.

• T1 (tryb dyskretny): Ten tryb wysyła pakiety co 15 sekund i, podobnie jak w trybie paranoicznym, żadne pakiety nie są wysyłane równolegle.

• T2 (tryb grzecznościowy): Ten tryb wysyła pakiet co 0,4 sekundy; ten tryb również nie wysyła pakietów równolegle. Ten tryb jest przydatny, gdy możliwości i obciążenie sieci są niepewne. Innymi słowy, pomaga zapobiegać blokowaniu lub zawieszaniu się sieci.

• T3 (tryb normalny): Ten tryb jest domyślny i nie wymaga zmiany, jeśli jest pożądany. Został zaprojektowany tak, aby działać szybko, nie obciążając sieci, a jednocześnie zapewniać szybkie informacje zwrotne. Ten tryb, podobnie jak kolejne, wykorzystuje skanowanie równoległe do zarządzania wynikami i szybkiego ich zwracania.

• T4 (tryb agresywny): Ten tryb nigdy nie będzie czekać na odpowiedź dłużej niż 1,25 sekundy przed wysłaniem kolejnego pakietu. Dokumentacja Nmapa sugeruje użycie opcji -T4 dla „rozsądnie nowoczesnych i niezawodnych sieci”.

• T5 (tryb szalony): Ten tryb czeka na odpowiedź na każde zapytanie nie dłużej niż 0,3 sekundy.

Dokumentacja sugeruje, że ten tryb powinien być używany tylko w bardzo szybkich sieciach. Dodatkowo, przy takim tempie, istnieje prawdopodobieństwo wystąpienia większej liczby błędów w wynikach, a także uruchomienia zabezpieczeń.

Przykład ustawienia szybkości skanowania może wyglądać następująco: sudo nmap -Pn -T5 -p1-500 192.168.255.2.

Nmap oferuje również bardziej precyzyjną kontrolę wykraczającą poza sześć wbudowanych prędkości, jeśli jest to konieczne. Ustawienia te nie są często używane; jednak jeśli Nmap jest używany przez personel bezpieczeństwa, manipulacja tymi polami może dodać wystarczająco charakterystyczną sygnaturę, dzięki której personel bezpieczeństwa mógłby odróżnić skanowanie autoryzowane od ataku, korzystając z narzędzia z domyślnymi ustawieniami. Bardziej szczegółowe opcje czasowe Nmap obejmują następujące:

• --host_timeout: Maksymalny czas w milisekundach spędzony na pojedynczym hoście przed przejściem dalej.

• --max_rtt_timeout: Maksymalny czas oczekiwania na odpowiedź sondy przed retransmisją

lub przekroczeniem limitu czasu. Wartość domyślna to 9000 milisekund.

• --min_rtt_timeout: Aby przyspieszyć skanowanie, Nmap mierzy czas reakcji celu i obniża limity czasu, dopasowując je do zachowania sieci tego celu, przyspieszając skanowanie, ale potencjalnie uniemożliwiając uzyskanie odpowiedzi w sieciach o dużej zmienności.

• --initial_rtt_timeout: Ta wartość ustawia początkowy limit czasu dla sond, który zostanie automatycznie obniżony, gdy Nmap zmierzy wydajność sieci docelowej. Wartość domyślna to 6000 milisekund.

• --max_parallelism: Ta opcja ustawia liczbę sond, które Nmap będzie wysyłał równolegle.

• --scan_delay: Ta wartość ustawia minimalny czas oczekiwania Nmapa między wysłaniem pakietów sond.

Przykład ustawienia szybkości skanowania może wyglądać następująco: sudo nmap –host-timeout 1 192.168.255.0/24.

Generowanie wyników

Nmap obsługuje parametry i funkcje wyjściowe serwera. Ten typ wyników staje się bardzo przydatny dla atakujących i obrońców do inwentaryzacji i kategoryzacji. Umożliwia on również wykorzystanie ich jako danych wejściowych do późniejszych skanów, raportów i innych narzędzi, które mogą wykorzystywać wyniki. Typy wyników i dodatkowe funkcje są wymienione poniżej:

• -oN/-oX/-oS/-oG <plik>: Wynik skanowania w następujących formatach – normalny, XML, s|<rIpt kIddi3 oraz format grepowalny, po którym następuje podana nazwa pliku

• -oA <nazwa_bazowa>: Wynik w trzech głównych formatach jednocześnie

• -v: Zwiększa poziom szczegółowości; Aby uzyskać jeszcze więcej szczegółów, użyj -vv

• -d[poziom]: Ustaw lub zwiększ poziom debugowania, zakres od 1 do 9

• --open: Pokaż tylko otwarte (lub potencjalnie otwarte) porty

• --packet-trace: Pokaż wszystkie wysłane i odebrane pakiety

• --iflist: Wyświetl interfejsy hosta i trasy (do debugowania)

• --log-errors: Rejestruj błędy/ostrzeżenia w pliku wyjściowym w normalnym formacie

• --append-output: Dodawaj zamiast nadpisywać określone dane wyjściowe

• --resume <nazwa_pliku>: Wznów przerwane skanowanie

• --stylesheet <ścieżka/URL>: Użyj arkusza stylów XSL do przekształcenia danych wyjściowych XML na HTML

• --webxml: Odwołaj się do arkusza stylów z nmap.org, aby uzyskać bardziej przenośny XML

• --no-stylesheet: Zapobiegaj kojarzeniu arkusza stylów XSL z danymi wyjściowymi XML

Przykładem użycia funkcji wyjściowej byłoby polecenie sudo nmap -Pn 192.168.255.2 -p1-1024 -oX scantarget.xml. To polecenie utworzy plik XML o nazwie scantarget.xml, który może być następnie wykorzystany przez inne narzędzia, w tym programy napisane na zamówienie, do wykonywania dalszych operacji. Jedną z przydatnych metod, z których korzystają osoby odpowiedzialne za obronę, jest wykorzystanie danych wyjściowych do bieżącego inwentaryzacji używanych maszyn i portów. W ten sposób można uzyskać dokładniejszą listę portów i usług, do szybkiego przeglądu, bez konieczności skanowania lub innego rodzaju rekonesansu. Teraz, gdy przyjrzeliśmy się danym wyjściowym, przyjrzyjmy się rozszerzeniu funkcji Nmapa poza jego podstawowe funkcje za pomocą NSE.

NSE

NSE ma wiele celów, które naprawdę rozszerzają możliwości Nmapa poza samo skanowanie portów i odciski palców systemu operacyjnego. Cele te obejmują:

• Wykorzystanie wydajnej, wielowątkowej architektury Nmapa do wysyłania dowolnych komunikatów i równoległego odbierania odpowiedzi do i z wielu systemów docelowych

• Stworzenie środowiska, w którym społeczność programistów może tworzyć i udostępniać darmowe skrypty, które mogą być łatwo włączane do skanowania przez wszystkich użytkowników Nmapa

• Obsługa opcji wykrywania sieci, które rozszerzają funkcje skanowania portów i odcisków palców systemu operacyjnego Nmapa, w tym wyszukiwanie Whois i przeszukiwanie DNS

• Rozszerzenie funkcji wykrywania wersji poza sondowanie i dopasowywanie, aby umożliwić głębszą analizę interakcji z systemem docelowym

• Przeprowadzanie skanowania podatności systemów docelowych w celu znalezienia luk w konfiguracji i innych problemów

• Wykrywanie systemów zainfekowanych złośliwym oprogramowaniem lub backdoorami na podstawie ich zachowania sieciowego

• Wspieranie wykorzystania luk w celu uzyskania dostępu do komputera docelowego lub jego danych; nie jest to funkcjonalność zintegrowana z Nmapem

Skrypty Nmapa są napisane w języku programowania Lua. Lua jest uważana za elastyczne i niezwykle szybkie środowisko skryptowe. Jej interpreter jest darmowy, wieloplatformowy i zajmuje bardzo mało miejsca. Lua została włączona do wielu projektów, w tym do open-source'owych systemów IDS Snort, Wireshark i RSA Netwitness do analizy ruchu sieciowego.

Wywołanie NSE można wykonać na kilka sposobów:

• Pierwszy sposób polega na użyciu przełącznika -sC, a następnie celu i portu. Spowoduje to uruchomienie skryptów w kategorii domyślnej, opisanej w kolejnym punkcie. Przykładem uruchomienia jest polecenie sudo nmap -sC 192.168.255.2 -p1-1024, które uruchamia skrypty na pierwszych 1024 portach adresu docelowego.

• Kolejnym sposobem wywołania NSE jest użycie kategorii. Twórcy skryptów podzielili skrypty na kilka kategorii, które są następujące:

- bezpieczne: Te skrypty zostały zaprojektowane tak, aby miały minimalny wpływ na cel.

- intruzywne: Te skrypty mogą pozostawiać wpisy w logu, próbować odgadnąć hasła, co skutkuje blokadami lub mieć inne skutki dla systemu.

- uwierzytelnianie: Skrypty w tej kategorii koncentrują się na procedurach uwierzytelniania i obejmują odgadywanie haseł oraz testy obejścia.

- malware: Te skrypty służą do sprawdzania obecności malware i backdoorów na obiekcie docelowym. Działania te obejmują sprawdzanie, czy popularny port backdoora nasłuchuje i działa. Inne działania obejmują przesłuchiwanie portów w celu uzyskania odpowiedzi powiązanych ze malware.

- version: Te skrypty próbują uzyskać informacje o wersji usług nasłuchujących na portach. Chociaż funkcja ta jest dostępna natywnie w Nmap, oferują one bardziej kompleksowe testy.

- discovery: Skrypty z tej kategorii służą do uzyskiwania dodatkowych informacji o środowisku sieciowym. Mogą one obejmować wyszukiwanie DNS i korzystanie z innych protokołów sieciowych prezentujących informacje o sieci.

- vuln: Te skrypty służą do określania, czy obiekt docelowy ma znaną lukę w zabezpieczeniach, taką jak niezałatana lub nieaktualna wersja, bądź błędna konfiguracja.

- external: Kategoria external wykorzystuje internetowe bazy danych i systemy innych firm do pobierania dodatkowych informacji. Mogą one obejmować takie elementy, jak wyszukiwanie Whois i geolokalizacja. - domyślne: Ta ostatnia kategoria obejmuje te same skrypty, które są uruchamiane po użyciu przełącznika -sC.

Przykład użycia kategorii NSE do skanowania to sudo nmap --script=safe192.168.255.2. Spowoduje to wykonanie wszystkich skryptów skategoryzowanych jako bezpieczne dla celu. Można również uwzględnić wiele kategorii, oddzielając je przecinkami. Zastosowanie tego do poprzedniego przykładu wyglądałoby tak: sudo nmap --script=safe,default 192.168.255.2. Tak jak poprzednio, spowoduje to wykonanie wszystkich skryptów w kategorii bezpiecznej, a także w kategoriach domyślnych. Na koniec, wybór skryptu NSE obsługuje wyrażenia and, or, a nie boolowskie, używając cudzysłowów i nawiasów do oddzielenia logiki; przykładem jest sudo nmap --script="(discovery and safe) and not smb*" 192.168.255.2. W tym przypadku uruchamiane są zarówno skrypty wykrywania, jak i bezpieczne, z wyjątkiem tych, które zaczynają się od smb. Ostatnim sposobem wywołania NSE jest wykorzystanie konkretnego skryptu. Format jest podobny do użycia filtra kategorii, z tą różnicą, że zamiast konkretnej kategorii podawana jest nazwa skryptu. Przykładem użycia konkretnego skryptu jest polecenie sudo nmap –script=http-auth.nse 192.168.255.2 -p80. Spowoduje to wykonanie skryptu http-auth.nse na obiekcie docelowym.

Kolejne oczywiste pytania brzmią: gdzie znajdują się te skrypty i jak uzyskać do nich dostęp? W systemach Windows katalog skryptów znajduje się w katalogu instalacyjnym Nmap. W systemach Linux katalog skryptów zazwyczaj znajduje się w katalogu /usr/share/nmap/scripts. W chwili pisania tego tekstu istnieje ponad 600 skryptów, które można wykorzystać z NSE. Wewnątrz katalogu znajduje się plik o nazwie scripts.db, który zawiera spis skryptów i powiązane z nimi kategorie; w ten sposób można również dowiedzieć się, które skrypty należą do jakich kategorii. Szybkim sposobem na to jest użycie polecenia grep w systemach Linux – na przykład polecenie grep version

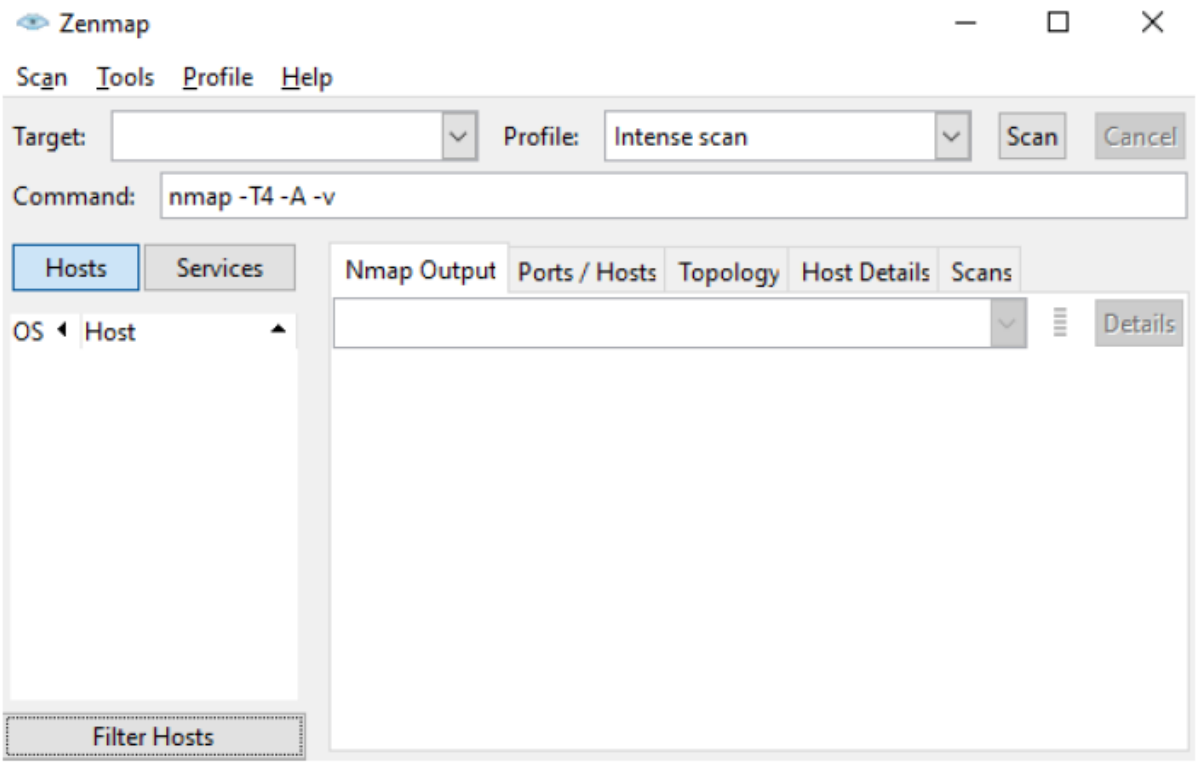
/usr/share/nmap/scripts/script.db wyświetli wszystkie skrypty należące do kategorii wersji. Przykład takiego wyniku można zobaczyć na poniższym zrzucie ekranu:

```
└─$ grep version /usr/share/nmap/scripts/script.db                                  2 ⚙
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version",
} }
Entry { filename = "bacnet-info.nse", categories = { "discovery", "version", } }
Entry { filename = "cccam-version.nse", categories = { "version", } }
Entry { filename = "db2-das-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "docker-version.nse", categories = { "version", } }
Entry { filename = "drda-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "enip-info.nse", categories = { "discovery", "version", } }
Entry { filename = "fingerprint-strings.nse", categories = { "version", } }
Entry { filename = "fox-info.nse", categories = { "discovery", "version", } }
Entry { filename = "freelancer-info.nse", categories = { "default", "discovery", "safe", "vers
ion", } }
Entry { filename = "hnap-info.nse", categories = { "default", "discovery", "safe", "version",
} }
Entry { filename = "http-cakephp-version.nse", categories = { "discovery", "safe", } }
```

Warto również zauważyć, że skrypty mogą należeć do więcej niż jednej kategorii. Skrypty napisane dla silnika NSE można również umieścić w katalogu scripts, aby zapewnić do nich łatwy dostęp. Plik script.db będzie wymagał aktualizacji, aby obsługiwał kategorie skryptów powiązanych z tymi skryptami. Należy jednak pamiętać, że wszelkie zmiany wprowadzone w tym folderze prawdopodobnie zostaną nadpisane po opublikowaniu nowych aktualizacji. Skoro omówiliśmy już wszystkie kwestie związane z wierszem poleceń Nmapa, przyjrzyjmy się interfejsowi graficznemu Nmapa.

Interfejs graficzny Nmapa

Jak wspomniano, Nmap posiada zarówno wiersz poleceń, jak i interfejs graficzny. Interfejs graficzny o nazwie Zenmap obsługuje kilka funkcji i konfiguracji. Ekran główny po uruchomieniu Nmapa można zobaczyć na poniższym zrzucie ekranu:



Niektóre z funkcji obejmują pole Cel, które obsługuje nazwy komputerów, pojedyncze adresy IP i podsieci. W menu rozwijanym Profil ustawiono 10 wstępnie skonfigurowanych typów skanowania, w tym następujące:

• Skanowanie intensywne: Ten profil dodaje parametr -T4 -A -v do celu skanowania

• Skanowanie intensywne plus UDP: Ten profil dodaje parametr -sS -sU -T4 -A -v do celu skanowania

• Skanowanie intensywne, wszystkie porty TCP: Ten profil dodaje parametr -p 1-65535 -T4 -A -v do celu skanowania

• Skanowanie intensywne, bez pingowania: Ten profil dodaje parametr -T4 -A -v -Pn do celu skanowania

• Skanowanie ping: Ten profil dodaje parametr -sn do celu skanowania

• Szybkie skanowanie: Ten profil dodaje parametr -T4 -F do celu skanowania

• Szybkie skanowanie plus: Ten profil dodaje parametr -sV -T4 -O -F –version-light do celu skanowania

• Szybkie traceroute: Ten profil dodaje parametr -sn –traceroute do celu skanowania

• Skanowanie regularne: Ten profil nie dodaje żadnych przełączników do celu skanowania

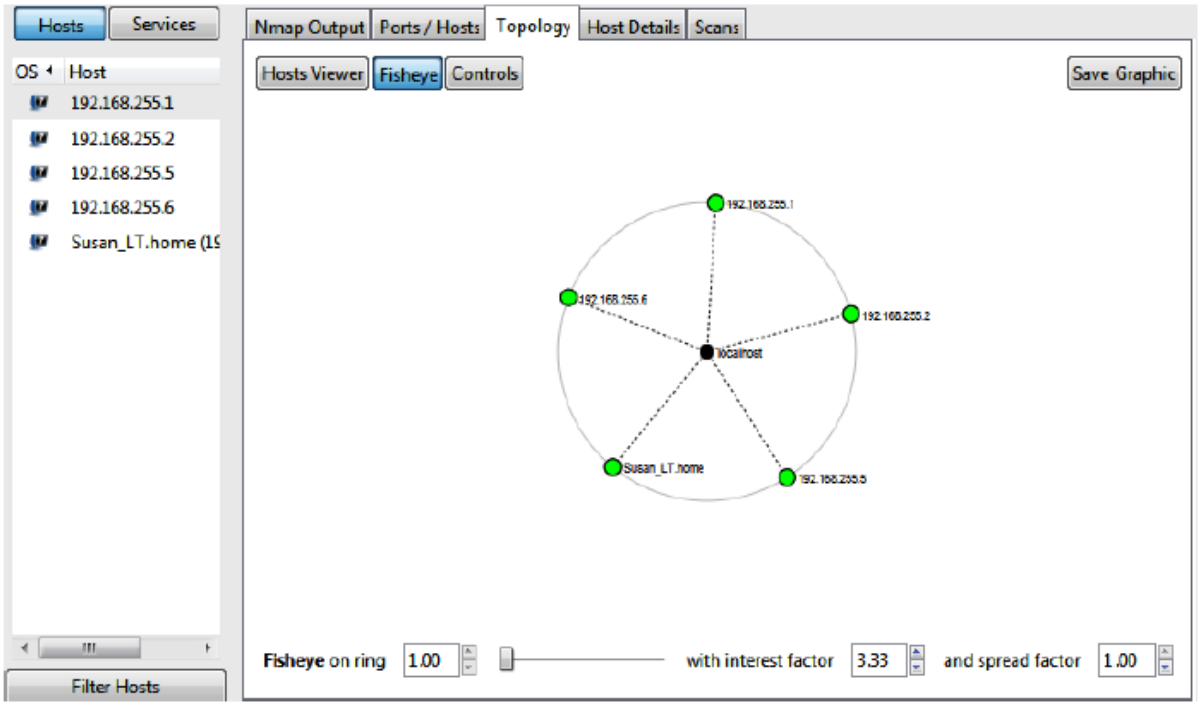
• Powolne skanowanie kompleksowe: Ten profil dodaje kilka przełączników, w tym -sS -sU -T4 -A

-v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53, do skanowanego obiektu.

Przyjrzyjmy się teraz pokrótce funkcji mapowania sieci w Zenmap.

Mapowanie sieci

Jedną z funkcji oferowanych przez Zenmap, której nie ma w wierszu poleceń, jest funkcja Topologia, która pozwala Zenmapowi na tworzenie wizualnej mapy sieci. Poniżej znajduje się przykład widoku Topologii w Zenmap:



Chociaż interfejs graficzny jest wygodny w użyciu, jest mniej elastyczny niż wersja wiersza poleceń, głównie dlatego, że nie można w nim łączyć innych poleceń i skryptów, takich jak zaplanowane zadania, przekierowywanie wyjść czy manipulacja, w zestaw zadań. Skoro poznaliśmy już zasady skanowania i enumeracji, poświęćmy trochę czasu na praktyczne zastosowanie tych informacji w laboratorium, korzystając z aplikacji Nmap.

Laboratorium – Skanowanie i enumeracja

Na początek uruchom środowisko laboratoryjne, w tym komputery Kali Linux i Metasploitable skonfigurowane w poprzednim laboratorium. Po uruchomieniu wszystkich komputerów zaloguj się na komputerze Kali, używającnazwy konta kali i hasła kali. Otwórz wiersz poleceń i uruchom następujące polecenia nmap na dostarczonych przełącznikach.

To ćwiczenie pokaże pingowanie i skanowanie portów TCP i UDP. Aby uzyskać wyjaśnienie działania przełączników, skorzystaj z podręcznika referencyjnego Nmap (http://nmap.org/book/man-riefoptions.html).

Aby lepiej to zrozumieć, po każdym z poniższych pytań podane jest polecenie lub polecenia, które należy uruchomić, aby uzyskać odpowiedź:

1. Wyjaśnij, co robi przełącznik -sn:

* Uruchom polecenie sudo nmap -sn 192.168.255.0/24

2. Wyjaśnij, co robi przełącznik –Pn:

* Uruchom polecenie sudo nmap –Pn 192.168.255.2

* Uruchom polecenie sudo nmap -Pn 192.168.255.3

3. Wyjaśnij, co robi przełącznik -sS:

* Uruchom polecenie sudo nmap -sS 192.168.255.2

* Uruchom polecenie sudo nmap -sS 192.168.255.3

4. Wyjaśnij, co robią przełączniki -sT i -sU:

* Uruchom polecenie sudo nmap –sT 192.168.255.2

* Uruchom polecenie sudo nmap –sU 192.168.255.2 polecenie

* Uruchom polecenie sudo nmap –sT 192.168.255.3

* Uruchom polecenie sudo nmap –sU 192.168.255.3

5. Wyjaśnij, co robi przełącznik -O:

* Uruchom polecenie sudo nmap –O 192.168.255.2

* Uruchom polecenie sudo nmap –O 192.168.255.3

6. Wyjaśnij, co robi przełącznik -sV:

* Uruchom polecenie sudo nmap -sV 192.168.255.2

* Uruchom polecenie sudo nmap -sV 192.168.255.3

7. Wyjaśnij, co robi przełącznik -A:

* Uruchom polecenie sudo nmap -A 192.168.255.2

* Uruchom polecenie sudo nmap -A Polecenie 192.168.255.3

8. Wyjaśnij, co robi przełącznik -p1-1024:

* Uruchom polecenie sudo nmap –Pn 192.168.255.2 -p1-1024

* Uruchom polecenie sudo nmap -Pn 192.168.255.3 -p1-1024

Skoro dotarliśmy już do końca tego rozdziału, podsumujmy pokrótce to, czego się nauczyliśmy.

Podsumowanie

omówiliśmy skanowanie i enumerację, pokazując, jak to się robi na poziomie podstawowym, przy użyciu wbudowanych narzędzi, takich jak Ping i Traceroute. Przedstawiliśmy również Nmap, który jest de facto standardowym narzędziem do skanowania. To solidne narzędzie potrafi nie tylko mapować sieci, ale także identyfikować otwarte porty i usługi, a dzięki silnikowi skryptowemu może wykonywać bardzo złożone techniki skanowania. Najlepsze jest to, że narzędzie to jest nie tylko dołączone do każdej instalacji Kali, ale jest również dostępne do pobrania za darmo dla każdego systemu operacyjnego. Później zagłębimy się w skanowanie, analizując luki w zabezpieczeniach i skanowanie podatności. Dodatkowo zobaczymy, jak obrońcy sieci wykorzystują uzyskane informacje do oceny podatności organizacji. Ten proces jest znany jako modelowanie zagrożeń lub ocena ryzyka.

Ocena

1. Jakiego protokołu używa narzędzie PING?

A. ARP

B. ICMP

C. MTTQ

D. NetBios

2. Co oznacza TTL w wynikach PING?

A. Talk to Little

B. Całkowity utracony czas

C. Czas życia (Time to Live)

D. Całkowity limit czasu

3. Jaka jest maksymalna liczba portów dostępnych na komputerze?

A. 1024

B. 20 480

C. 65 535

D. 128 000

4. Czym jest również skanowanie TCP SYN?

A. Skanowanie choinkowe

B. Skanowanie negatywne

C. Skanowanie flagowe

D. Skanowanie półotwarte

5. Wszystkie problemy są związane ze skanowaniem portów, z wyjątkiem:

A. Fałszywie pozytywnego wyniku

B. Fałszywie negatywnego wyniku

C. Podsieci

D. Niezarejestrowanych numerów portów

6. Który przełącznik Nmap wykonuje tylko operację ping? A. -sS

B. -sV

C. -sP

D. -A

7. Jakiego języka używa język skryptowy Nmap?

A. C

B. Lua

C. Python

D. Fortran

8. Co robi narzędzie Traceroute?

A. Maszyny docelowe ataków DDoS (Distributed Denial of Service)

B. Śledzi sieć

C. Mapuje routery

D. Optymalizuje trasy sieciowe

9. NSE ma następujące kategorie skryptów, z wyjątkiem:

A. Intruzyjnych

B. Obraźliwych

C. Zewnętrznych

D. Złośliwego oprogramowania

10. Jak nazywa się wersja Nmap z graficznym interfejsem użytkownika?

A. SYNmap

B. NMap GTK

C. NMapGUI

D. Zenmap

Odpowiedź

1. B

2. C

3. C

4. D

5. D

6. C

7. B

8. C

9. D

10. D