LUKI W ZABEZPIECZENIACH SYSTEMÓW OPERACYJNYCH NA STACJONARNYCH I SERWERACH

Nauczyłeś się, jak enumerować systemy, aby odkryć otwarte porty, które mogą być używane do uzyskiwania dostępu do danych i zasobów. Po enumeracji systemów, Twoim zadaniem jako testera bezpieczeństwa jest wskazanie potencjalnych problemów bezpieczeństwa. Musisz również znać metody poprawy bezpieczeństwa w testowanych systemach i naprawiania lub minimalizowania ryzyka stwarzanego przez te luki w zabezpieczeniach. Ten moduł bada, jak używać testów bezpieczeństwa do analizowania systemu operacyjnego pod kątem luk w zabezpieczeniach i ich korygowania. Na koniec poznasz techniki i najlepsze praktyki wzmacniania systemów operacyjnych i usług.

LUKI W ZABEZPIECZENIACH SYSTEMÓW OPERACYJNYCH WINDOWS

Wiele systemów operacyjnych Windows ma poważne luki w zabezpieczeniach. We wczesnych wersjach systemu Windows, w tym Windows 2000 i starszych, kilka usług i funkcji było niezabezpieczonych i otwartych do dostępu. Aby zabezpieczyć te systemy, administratorzy muszą wyłączyć, ponownie skonfigurować lub odinstalować usługi i funkcje, aby zmniejszyć ich podatność na ataki. Aby poprawić bezpieczeństwo, nowsze wersje systemu Windows domyślnie wyłączają większość usług i funkcji. W tych środowiskach administratorzy muszą skonfigurować niezbędne usługi i funkcje, aby były dostępne, w przeciwnym razie użytkownicy nie będą mogli uzyskać dostępu do potrzebnych im zasobów. Krótko mówiąc, bezpieczeństwo jest bardziej rygorystyczne w tych późniejszych wersjach. Jednak gdy usługi nie są dostępne, użytkownicy często nie mogą wykonywać swoich zadań. Cały moduł można by poświęcić temu problemowi, ale na razie pamiętaj, że duża część bezpieczeństwa informacji w środowisku korporacyjnym polega na znalezieniu równowagi między użytecznością a bezpieczeństwem. Aby znaleźć luki w zabezpieczeniach dla dowolnego systemu operacyjnego, możesz sprawdzić witryny internetowe dotyczące luk CVE i CERT (www.cve.mitre.org i www.kb.cert.org/vuls). Tabela 8-1 krótko opisuje kilka luk CVE dla systemu Windows Server 2019 i pokazuje, w jaki sposób luka w zabezpieczeniach jednej wersji systemu operacyjnego może mieć zastosowanie również do innych wersji. Wiele wyjaśnień na stronie internetowej CVE jest złożonych i może być trudnych do zrozumienia. Powinieneś jednak być w stanie zbadać lukę w zabezpieczeniach, która jest istotna dla przeprowadzanego testu bezpieczeństwa. Na przykład, jeśli system, który testujesz, używa Menedżera połączeń dostępu zdalnego wymienionego w CVE-2021-33763, być może będziesz musiał przeprowadzić badanie dotyczące tego, czym jest Menedżer połączeń dostępu zdalnego (usługa systemu Windows, która zarządza połączeniami wirtualnej sieci prywatnej) i czy wersja, na której działa dany serwer, jest podatna na atak. Być może będziesz musiał również odwiedzić stronę internetową firmy Microsoft, aby sprawdzić, czy są dostępne jakieś poprawki lub aktualizacje zabezpieczeń dla tej luki w zabezpieczeniach. Na przykład wyszukiwanie „CVE-2021-33763” w Google ujawnia kilka wyników. Jeśli klikniesz na link https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33763, zostaniesz przeniesiony do szczegółów Microsoft Security Update Guide dla tej luki, gdzie możesz pobrać listę aktualizacji zabezpieczeń, aby załatać różne wersje systemu Windows. Testerzy bezpieczeństwa mogą wykorzystać informacje z witryny CVE do przetestowania komputera z systemem Windows i upewnić się, że został on załatany aktualizacjami firmy Microsoft, które usuwają te znane luki. Hakerzy odwiedzają witryny oferujące programy wykorzystujące luki w zabezpieczeniach, ale luki powinny być używane tylko w określonych przypadkach, a jako etyczny haker musisz uzyskać wcześniejszą zgodę. Innymi słowy, nie chcesz demontować systemu, aby zademonstrować luki w zabezpieczeniach firmy; chcesz poinformować firmę, gdy jej systemy są podatne na ataki. Wiele z tych znanych luk znajduje się na portach, które narzędzia do skanowania portów mogą łatwo wykryć jako otwarte porty. Na przykład SMB (tcp/139 lub tcp/445), SMTP (tcp/25), HTTPS (tcp/443) i RPC (tcp/135) mogą być podatne na ataki. Narzędzia takie jak Nessus i OpenVAS pomagają zautomatyzować identyfikację luk w zabezpieczeniach, ale upewnij się, że rozumiesz wyniki, jakie każde narzędzie

zapewnia, wykonując dalsze badania. Podczas prowadzenia badań zrób coś więcej niż tylko pobieżne przejrzenie informacji CVE. Pamiętaj, że dbałość o szczegóły odróżnia wykwalifikowanych testerów bezpieczeństwa od przeciętnych. Większość luk w zabezpieczeniach jest wynikiem drobnych błędów lub pominięć w kodzie lub ustawieniach konfiguracji, które mogą skutkować poważnymi problemami bezpieczeństwa.

Systemy plików Windows

Celem każdego systemu plików, niezależnie od systemu operacyjnego, jest przechowywanie i zarządzanie informacjami. System plików organizuje informacje tworzone przez użytkowników, a także pliki systemu operacyjnego potrzebne do uruchomienia systemu, więc system plików jest najważniejszą częścią każdego systemu operacyjnego. W niektórych przypadkach ten krytyczny komponent systemu operacyjnego może być podatny na ataki.

Tabela alokacji plików

Tabela alokacji plików (FAT), oryginalny system plików firmy Microsoft, jest obsługiwany przez niemal wszystkie systemy operacyjne komputerów stacjonarnych i serwerów od 1981 r. do dziś. Późniejsze wersje, takie jak FAT16, FAT32 i Extended FAT (exFAT, opracowany dla systemu Windows Embedded CE), zapewniają większe rozmiary plików i dysków. Na przykład FAT32 pozwala, aby pojedynczy plik zawierał do 4 GB danych, a wolumin dysku zawierał do 8 terabajtów (TB). Ze względu na szerokie wsparcie FAT32 jest również standardowym systemem plików dla większości nośników wymiennych innych niż płyty CD i DVD. Najpoważniejszą wadą FAT jest to, że nie obsługuje list kontroli dostępu na poziomie plików (ACL), które są niezbędne do ustawiania uprawnień do plików. Z tego powodu używanie FAT w środowisku wielodostępnym powoduje krytyczną lukę w zabezpieczeniach. Microsoft zajął się tym problemem i innymi niedociągnięciami FAT, wprowadzając swój pierwszy system operacyjny dla przedsiębiorstw, Windows NT.

NTFS

System plików New Technology File System (NTFS) został po raz pierwszy wydany jako system plików klasy high-end w systemie Windows NT 3.1, a w systemie Windows NT 3.51 dodano obsługę większych plików i woluminów dyskowych, a także zabezpieczenia plików ACL. Późniejsze wersje systemu Windows zawierały uaktualnienia dotyczące kompresji, kwot dyskowych, dzienników, szyfrowania na poziomie plików, transakcyjnego NTFS, łączy symbolicznych i samonaprawiania. NTFS jest obecnie używany w systemach Windows 10. Jednak nawet przy silnych funkcjach bezpieczeństwa NTFS ma pewne wrodzone luki w zabezpieczeniach; niektórzy mogą nazywać te luki funkcjami. Na przykład jedną mało znaną funkcją NTFS są alternatywne strumienie danych (ADS), napisane dla zgodności z Apple Hierarchical File System (HFS). ADS może przesyłać strumieniowo (ukrywać) informacje za istniejącymi plikami bez wpływu na ich funkcję, rozmiar lub inne informacje, co umożliwia intruzom systemu ukrywanie narzędzi do eksploatacji i innych złośliwych plików. Do wykrywania ADS można użyć kilku metod. W systemie Windows Vista i nowszych do polecenia dir dodano przełącznik: Wprowadź dir /r z katalogu, który chcesz przeanalizować, aby wyświetlić wszystkie ADS. W przypadku poprzednich wersji systemu Windows należy pobrać narzędzie, takie jak Streams.exe ze strony https://technet.microsoft.com/en-us/sysinternals/bb897440.aspx. Bez względu na zastosowaną metodę należy ustalić, czy wykryte ADS powinny się tam znajdować. Lepszą i wydajniejszą metodą wykrywania złośliwych zmian w systemie plików jest użycie narzędzi do monitorowania integralności plików opartych na hoście, takich jak Tripwire (www.tripwire.com) lub Log-Rhythm (www.logrhythm.com). Dostępna jest również wersja Tripwire oparta na *nix.

Zdalne wywołanie procedury

Zdalne wywołanie procedury (RPC) to mechanizm komunikacji międzyprocesowej, który umożliwia programowi działającemu na jednym hoście uruchomienie kodu na hoście zdalnym. Robak Conficker wykorzystał lukę w zabezpieczeniach RPC do uruchomienia dowolnego kodu na podatnych hostach. Biuletyn zabezpieczeń firmy Microsoft MS08-067, opublikowany 23 października 2008 r., poinformował użytkowników o tej krytycznej luce, która umożliwiała atakującym uruchomienie własnego kodu, i zaoferował poprawkę w celu naprawienia problemu. Mimo że luka została opublikowana w poradnikach, a poprawka była dostępna na kilka tygodni przed atakiem robaka Conficker 21 listopada 2008 r., miliony komputerów zostało dotkniętych. Stuxnet, który pojawił się w 2010 r., wykorzystał tę samą lukę, której Conficker użył do rozprzestrzeniania swojej infekcji trzy lata wcześniej. Nessus to doskonałe narzędzie do określania, czy system jest podatny na problem związany z RPC, a także do wielu innych elementów konfiguracji i łatania. W Aktywności 8-1 pobierasz i instalujesz Nessus Essentials na swoim komputerze z systemem Windows. Jeśli zainstalowałeś już Nessus Essentials, możesz pominąć tę aktywność.

Pobieranie i instalowanie Nessus Essentials

Czas trwania: 30 minut

Cel: Pobranie i zainstalowanie Nessus Essentials.

Opis: W tej aktywności pobierasz i instalujesz Nessus Essentials, popularne narzędzie do skanowania luk w zabezpieczeniach, służące do wykrywania luk w zabezpieczeniach systemów Windows i Linux. Nessus Essentials to darmowa wersja Nessus. Ma taką samą funkcjonalność jak komercyjny produkt Nessus Professional, ale ogranicza liczbę adresów IP, z którymi możesz pracować.

1. W systemie Windows uruchom przeglądarkę internetową i przejdź na stronę www.tenable.com/downloads/nessus. Aby zainstalować Nessus Essentials, potrzebujesz kodu aktywacyjnego, więc możesz kliknąć łącze lub przycisk na stronie pobierania, aby go uzyskać. Masz również inną możliwość uzyskania kodu aktywacyjnego później w krokach instalacji. Kod aktywacyjny zostanie wysłany na podany przez Ciebie adres e-mail.

2. Kliknij odpowiedni link pobierania dla swojego systemu operacyjnego. Jeśli używasz systemu Windows, najprawdopodobniej używasz 64-bitowej wersji systemu Windows, więc wybierz Nessus-8.15.0-x64.msi.

3. Po zakończeniu pobierania przejdź do lokalizacji zapisanego pliku i kliknij dwukrotnie plik wykonywalny instalatora. Jeśli zobaczysz komunikat ostrzegawczy, kliknij przycisk Uruchom lub OK, aby kontynuować. Otworzy się okno Kreatora InstallShield.

4. Zamknij wszystkie uruchomione aplikacje systemu Windows, a następnie kliknij przycisk Dalej.

5. Postępuj zgodnie z instrukcjami i zaakceptuj umowy licencyjne oraz ustawienia domyślne, chyba że instruktor zaleci inaczej.

6. Po zakończeniu instalacji domyślna przeglądarka internetowa otworzy stronę Witamy w instalacji Nessus. Kliknij przycisk Połącz przez SSL.

7. Na stronie Witamy w Nessus kliknij Nessus Essentials, a następnie kliknij przycisk Kontynuuj.

8. Gdy zostaniesz poproszony o podanie kodu aktywacyjnego, wprowadź kod, a następnie kliknij przycisk Kontynuuj. Nessus Essentials kończy instalację i zaczyna pobierać wtyczki potrzebne do wykonywania skanów podatności.

9. Aby uruchomić Nessus Essentials w przyszłości, otwórz kartę przeglądarki internetowej i wprowadź https://localhost:8834. Będziesz używać Nessus Essentials w nadchodzącej aktywności.

NetBIOS

Przypomnijmy, że NetBIOS to oprogramowanie ładowane do pamięci, które umożliwia programowi interakcję z zasobem sieciowym lub urządzeniem. Zasoby sieciowe są identyfikowane za pomocą 16-bajtowych nazw NetBIOS. NetBIOS nie jest protokołem; jest interfejsem protokołu sieciowego, który umożliwia programowi dostęp do zasobu sieciowego. Zwykle działa z rozszerzonym interfejsem użytkownika NetBIOS (netbeui), szybkim, wydajnym protokołem, który wymaga niewielkiej konfiguracji i umożliwia przesyłanie pakietów NetBIOS przez TCP/IP i różne topologie sieciowe. NetBIOS przez TCP/IP jest domyślnie wyłączony w obecnych wersjach systemu Windows, ale był domyślnie włączony przed systemami Windows Vista i Server 2008. Systemy z nowszymi systemami operacyjnymi Windows mogą udostępniać pliki i zasoby bez korzystania z NetBIOS; jednak NetBIOS jest nadal używany ze względu na wsteczną zgodność, co jest ważne, gdy budżety organizacji nie pozwalają na uaktualnienie każdego komputera w sieci. Ponadto należy spełnić oczekiwania klientów. Na przykład klienci oczekują, że dokument utworzony w programie Word 2010 nadal będzie można odczytać w programie Word 2019. W rzeczywistości tego wymagają. Dlatego twórcy oprogramowania stają przed wyzwaniem poprawy bezpieczeństwa systemu operacyjnego przy jednoczesnym zapewnieniu zgodności z mniej bezpiecznymi poprzednikami. Dopóki nowsze systemy operacyjne Windows muszą współpracować ze starszymi systemami opartymi na NetBIOS, bezpieczeństwo będzie wyzwaniem.

Blok komunikatów serwera

W systemie Windows blok komunikatów serwera (sMb) jest używany do udostępniania plików i zwykle działa na NetBIOS, NetBEUI lub TCP/IP. Kilka narzędzi hakerskich, których celem jest SMB, nadal może powodować uszkodzenia sieci Windows. Dwa dobrze znane narzędzia hakerskie SMB to narzędzie L0phtcrack SMB Packet Capture i SMBRelay, które przechwytują ruch SMB i zbierają nazwy użytkowników i skróty haseł. Co ciekawe, Microsoft potrzebował siedmiu lat, aby załatać lukę w zabezpieczeniach, którą wykorzystywały te narzędzia hakerskie. Wielu badaczy bezpieczeństwa wskazuje na tę sytuację jako na kolejny przykład problemu spowodowanego zapewnieniem wstecznej kompatybilności. Kontynuując korzystanie z protokołu ze znaną luką w zabezpieczeniach (którą można również opisać jako wadę konstrukcyjną), Microsoft naraża swoje produkty na ataki i wykorzystanie. Microsoft wprowadził SMB2 w systemie Windows Vista, SMB3 w systemie Windows 8 i SMB3.1.1 w systemie Windows 10. Każda nowa wersja SMB naprawiała problemy z zabezpieczeniami i często dodawała funkcje i ulepszenia wydajności. Luki w zabezpieczeniach SMB są powszechnym wektorem ataku wykorzystywanym przez złośliwe oprogramowanie. Robaki, na przykład, wyszukują udziały SMB i próbują użyć podatnych udziałów, aby kopiować się z komputera na komputer przez sieć.

Common Internet File System

Common Internet File System (CIFS) to standardowy protokół, który zastąpił SMB w systemie Windows 2000 Server, ale aby zapewnić wsteczną zgodność, nadal używano oryginalnego SMB.

UWAGA

CIFS jest obecnie uważany za przestarzały, a zamiast niego zwykle używa się SMBv3. Jednak CIFS może być nadal używany w niektórych starszych systemach lub jako metoda udostępniania plików między systemami Linux/Unix i Windows.

CIFS to protokół zdalnego systemu plików, który umożliwia komputerom udostępnianie zasobów sieciowych przez Internet. Innymi słowy, pliki, foldery, drukarki i inne zasoby mogą być udostępniane użytkownikom w całej sieci. Aby udostępnianie mogło mieć miejsce, sieć musi mieć infrastrukturę umożliwiającą umieszczanie tych zasobów w sieci oraz metodę kontrolowania dostępu do zasobów. CIFS opiera się na innych protokołach, aby obsługiwać ogłoszenia usługowe informujące użytkowników, jakie zasoby są dostępne w sieci, oraz obsługiwać uwierzytelnianie i autoryzację dostępu do tych zasobów. CIFS jest również dostępny dla wielu systemów *nix. Usługi Network Neighborhood lub My Network Places wykorzystują protokoły rozgłoszeniowe, aby ogłaszać zasoby dostępne w sieci. Zasadniczo komputer woła przez połączenie sieciowe „Oto jestem! Moja nazwa NetBIOS to Salesmgr i mam wiele plików i folderów do udostępnienia każdemu". Aby udostępniać pliki i foldery, CIFS opiera się na protokole SMB, ale oferuje wiele udoskonaleń, w tym:

• Funkcje blokowania, które umożliwiają wielu użytkownikom dostęp do pliku i jego aktualizację jednocześnie bez konfliktów

• Buforowanie i możliwość odczytu z wyprzedzeniem/zapisu z opóźnieniem

• Obsługa tolerancji błędów

• Możliwość wydajniejszej pracy na wolnych łączach dial-up

• Obsługa anonimowego i uwierzytelnionego dostępu do plików w celu zwiększenia bezpieczeństwa. Aby zapobiec nieautoryzowanemu dostępowi do tych plików, CIFS opiera się na modelu bezpieczeństwa protokołu SMB. Administrator może wybrać dwie metody zabezpieczeń serwera:

• Zabezpieczenia na poziomie udziału — folder na dysku jest udostępniany użytkownikom do udostępniania. Można skonfigurować hasło dla udziału, ale nie jest to wymagane.

• Zabezpieczenia na poziomie użytkownika — zasób jest udostępniany użytkownikom sieci; jednak do uzyskania dostępu do zasobu wymagana jest nazwa użytkownika i hasło. Serwer SMB przechowuje zaszyfrowaną wersję haseł użytkowników w celu zwiększenia bezpieczeństwa.

Nowsze wersje systemu Windows Server nasłuchują na większości tych samych portów, co starsze wersje, co oznacza, że wiele starych ataków może nadal działać na nowszych systemach operacyjnych. Na przykład, rozpoznając, które porty są otwarte w systemie Windows Server, tester bezpieczeństwa może znaleźć luki, które umożliwiają wprowadzenie trojana lub innego programu zdalnego sterowania w celu przechwycenia haseł i nazw logowania autoryzowanych użytkowników. Większość atakujących szuka serwerów wyznaczonych jako kontrolery domeny (serwery obsługujące uwierzytelnianie). Kontrolery domeny Windows są używane do uwierzytelniania kont użytkowników, więc zawierają większość informacji, do których atakujący chcą uzyskać dostęp. Domyślnie kontrolery domeny Windows nasłuchują na następujących portach:

• DNS (port 53)

• HTTP (port 80)

• Kerberos (port 88)

• RPC (port 135)

• Usługa nazw NetBIOS (port 137)

• Usługa datagramów NetBIOS (port 139)

• LDAP (port 389)

• HTTPS (port 443)

• SMB/CIFS (port 445)

• LDAP przez SSL (port 636)

• Katalog globalny Active Directory (port 3268)

Kontrolery domeny Windows są zwykle również serwerami globalnego katalogu (GC). Globalne serwery katalogu są używane do lokalizowania zasobów w domenie zawierającej tysiące, a nawet miliony obiektów. Na przykład, jeśli użytkownik chce zlokalizować drukarkę ze słowem „color" w opisie, domena wysyła zapytanie do serwera GC, który zawiera atrybuty, takie jak nazwa i lokalizacja zasobu, i kieruje użytkownika do zasobu sieciowego.

Sesje zerowe

Przypomnijmy, że sesja zerowa to anonimowe połączenie nawiązane bez danych uwierzytelniających, takich jak nazwa użytkownika i hasło. Nazywana również logowaniem anonimowym, sesja zerowa może być używana do wyświetlania informacji o użytkownikach, grupach, udziałach i zasadach haseł. Sesje zerowe są konieczne tylko wtedy, gdy sieci muszą obsługiwać starsze wersje systemu Windows. Niemniej jednak wiele organizacji nadal ma włączone sesje zerowe, mimo że wszystkie ich stare systemy Windows zostały usunięte z sieci. Możesz użyć poleceń Nbtstat, Net view, Netstat, Ping, Pathping i Telnet, aby wyliczyć zagrożenia NetBIOS.

Usługi sieciowe

Starsze wersje usług sieciowych i IIS domyślnie włączały wiele funkcji, pozostawiając systemy z dużą powierzchnią ataku. Firma Microsoft opracowała Kreatora blokady IIS specjalnie do blokowania wersji IIS 4.0 i 5.0. Jednak jako tester bezpieczeństwa powinieneś zachęcać klientów do uaktualniania dowolnego systemu operacyjnego i oprogramowania, które nie jest już obsługiwane, zamiast korzystania z obejść zabezpieczeń, takich jak Kreator blokady IIS. IIS 5.0 jest instalowany domyślnie w systemie Windows 2000 Server, co oznacza, że serwer Windows 2000 jest również serwerem internetowym korzystającym z domyślnej konfiguracji, konfiguracji, o której wielu administratorów nie wie, dopóki nie wystąpi problem. Windows 2000 to starszy system operacyjny, a prawdopodobieństwo natrafienia na instalację nadal działającą w organizacji jest bardzo małe, ale sednem sprawy jest to, aby nie zakładać, że w sieci nie ma serwera internetowego tylko dlatego, że nie zainstalowano go specjalnie. Chociaż IIS 6.0 (Windows Server 2003) do IIS 10.0.17763 (Windows Server 2019) są instalowane w trybie „domyślnie bezpiecznym", poprzednie wersje pozostawiły kluczowe luki, które umożliwiały atakującym wślizgnięcie się do sieci. Niezależnie od wersji IIS, na której działa system, ważne jest, aby systemy były łatane, a administratorzy systemów powinni nadal wiedzieć, jakie poprawki są instalowane i które usługi są uruchomione na ich serwerach internetowych. Konfigurowanie tylko niezbędnych usług i aplikacji to mądre posunięcie.

MS SQL Server

Starsze wersje Microsoft SQL Server mają wiele potencjalnych luk, których nie można szczegółowo omówić w tym kursie. Najczęstszą krytyczną luką w zabezpieczeniach SQL jest puste hasło SA. Wszystkie wersje przed SQL Server 2005 mają lukę, która może umożliwić użytkownikom zdalnym uzyskanie dostępu administratora systemu (SA) za pośrednictwem konta SA na serwerze. Podczas instalacji SQL Server 6.5 i 7 użytkownik jest proszony — ale nie jest to wymagane — o ustawienie hasła na tym koncie. SQL Server 2000 domyślnie używa uwierzytelniania zintegrowanego systemu Windows, ale użytkownik może również wybrać uwierzytelnianie w trybie mieszanym. W tym trybie

uwierzytelniania tworzone jest konto SA z pustym hasłem, którego nie można wyłączyć. Jeśli atakujący znajdą to konto, uzyskają dostęp administracyjny nie tylko do bazy danych, ale potencjalnie także do serwera bazy danych. Jest mało prawdopodobne, że natkniesz się na instalację SQL Server wystarczająco starą, aby mieć tę lukę, ale serwery często używają ustawień domyślnych, a niektóre z tych ustawień domyślnych sprawiają, że serwery Windows są podatne na ataki. Skanery podatności, takie jak Nessus i OpenVAS, nadal skanują w poszukiwaniu tej luki w zabezpieczeniach serwera SQL.

Przepełnienia bufora

Przypomnijmy, że przepełnienie bufora występuje, gdy dane są zapisywane do bufora (tymczasowej przestrzeni pamięci) i z powodu niewystarczającego sprawdzania granic uszkadzają dane w pamięci obok przydzielonego bufora. Zwykle ten problem występuje, gdy niebezpieczne funkcje używają danych wejściowych, które nie zostały prawidłowo zweryfikowane. Z powodu wad projektowych kilka funkcji nie weryfikuje, czy akceptowane przez nie liczby lub ciągi mieszczą się w buforze dostarczonym do ich przechowywania. Jeśli ten brak weryfikacji zostanie wykorzystany, może to umożliwić atakującym uruchomienie kodu powłoki. Zarówno C, jak i C++ nie mają wbudowanej ochrony przed nadpisywaniem danych w pamięci, więc aplikacje napisane w tych językach są podatne na ataki przepełnienia bufora. Ponieważ te języki programowania są szeroko stosowane, luki w zabezpieczeniach przepełnienia bufora są powszechne w wielu aplikacjach i systemach operacyjnych. Ataki przepełnienia bufora nie wymagają uwierzytelnionego użytkownika i mogą być przeprowadzane zdalnie. Na szczęście nowoczesne frameworki programistyczne obejmują procedury dezynfekujące i inne funkcje bezpieczeństwa, które pomagają programistom kodować bezpieczniej. Jednak to nadal od programisty zależy, czy użyje tych funkcji, aby stworzyć bezpieczny kod.

Hasła i uwierzytelnianie

Już wiesz, że najsłabszym ogniwem bezpieczeństwa w każdej sieci są autoryzowani użytkownicy. Niestety, to ogniwo jest najtrudniejsze do zabezpieczenia, ponieważ opiera się na osobach, które mogą nie zdawać sobie sprawy, że ich działania mogą narazić ich organizację na poważne naruszenie bezpieczeństwa, skutkujące uszkodzeniem systemów, kradzieżą lub zniszczeniem informacji, infekcją złośliwym oprogramowaniem itd. Po ataku mogą również pojawić się problemy prawne, z którymi należy się uporać, a firma może w rezultacie stracić zaufanie klientów. Firmy powinny podjąć kroki w celu rozwiązania tej luki w zabezpieczeniach. Kompleksowa polityka haseł ma kluczowe znaczenie, ponieważ nazwa użytkownika i hasło są często wszystkim, co dzieli atakującego od dostępu. Polityka haseł powinna obejmować następujące elementy:

• Regularna zmiana haseł na kontach na poziomie systemu.

• Wymaganie od użytkowników zmiany haseł co kwartał. Chociaż może to być rozsądna praktyka, którą zaleca wielu specjalistów ds. bezpieczeństwa, niektóre organizacje ds. bezpieczeństwa sugerują, że częste zmiany haseł powodują, że hasła są mniej bezpieczne, ponieważ użytkownicy mają tendencję do zmiany haseł w przewidywalny sposób, na przykład stopniowo zmieniając numer. Ponadto częste zmiany haseł mogą zachęcać użytkowników do używania tego samego hasła do różnych logowań. Dlatego organizacje te zasugerowały usunięcie wymogu zmiany hasła.

• Wymagaj minimalnej długości hasła wynoszącej co najmniej osiem znaków (i 15 znaków dla kont administracyjnych).

• Wymagaj złożonych haseł; innymi słowy, hasła muszą zawierać zarówno wielkie, jak i małe litery, cyfry, symbole i znaki interpunkcyjne. Jednak niektóre organizacje ds. bezpieczeństwa sugerują, że dłuższe hasła są lepsze od złożonych haseł. Hakerzy i ich zautomatyzowane narzędzia mogą odgadnąć

podstawienia $ za S lub @ za A, więc ten typ złożoności nie zwiększa bezpieczeństwa. Ponieważ złamanie dłuższych haseł zajmuje więcej czasu, eksperci ds. bezpieczeństwa sugerują porzucenie złożoności na rzecz długości.

• Hasła nie mogą być powszechnymi słowami, słowami znalezionymi w słowniku (w dowolnym języku) ani slangiem, żargonem lub dialektem.

• Hasła nie mogą być utożsamiane z konkretnym użytkownikiem, takimi jak daty urodzin, imiona lub słowa związane z firmą.

• Nigdy nie zapisuj hasła ani nie przechowuj go online lub w pliku na komputerze użytkownika. • Nie zdradzaj nikomu hasła przez telefon, e-mail ani osobiście.

• Wymagaj od użytkowników zachowania ostrożności podczas logowania, aby upewnić się, że nikt nie zobaczy, jak wprowadzają hasło.

• Ogranicz ponowne używanie starych haseł.

Oprócz tych wytycznych administratorzy mogą skonfigurować kontrolery domeny w celu wymuszenia wieku, długości i złożoności hasła. Na kontrolerach domeny systemu Windows można wymusić niektóre aspekty zasad dotyczących haseł, takie jak:

• Próg blokady konta — ustaw liczbę nieudanych prób, zanim konto zostanie tymczasowo wyłączone.

• Czas trwania blokady konta — ustaw okres czasu, w którym konto użytkownika jest zablokowane po określonej liczbie nieudanych prób logowania.

Na kontrolerach domeny systemu Windows Server 2008 i nowszych można wymusić wiele zasad dotyczących haseł. Na przykład jedna zasada dotycząca haseł może wymagać złożonego hasła składającego się z 15 lub więcej znaków dla kont administratorów, a inna zasada dotycząca haseł może wymagać tylko ośmiu znaków dla kont użytkowników bez uprawnień administracyjnych. Pomimo wszelkich starań w celu promowania bezpieczeństwa poprzez wymuszanie zasad dotyczących haseł, hasło nadal może zostać złamane. Najnowsze narzędzia, które zawierają tabele tęczowe, mogą łamać złożone hasła zaskakująco szybko. Więcej szczegółów na temat łamania haseł znajdziesz w późniejszym module.

NARZĘDZIA DO IDENTYFIKOWANIA LUK W SYSTEMIE WINDOWS

Dostępnych jest wiele narzędzi do wykrywania luk w systemie Windows. Zalecane jest korzystanie z więcej niż jednego narzędzia do analizy, więc nauka różnych metod i narzędzi jest korzystna dla Twojej kariery. Znajomość kilku narzędzi pomaga również dokładniej lokalizować problemy. Niektóre narzędzia mogą raportować mylące wyniki, a jeśli wyniki te nie zostaną zweryfikowane inną metodą, możesz nie mieć dokładnej oceny do raportowania. Popularne skanery luk w systemie operacyjnym to Tripwire IP360, Tenable Nessus, Nexpose i OpenVAS. W poprzednich modułach zapoznałeś się z Nessus i OpenVAS. Wszystkie te produkty skanują zarówno systemy operacyjne Linux, jak i Windows. Ponadto kilka narzędzi jest specjalnie zaprojektowanych dla systemu Windows. W poniższej sekcji zapoznasz się z wykorzystaniem Nessus do oceny systemów Windows.

Skanowanie systemu Windows za pomocą Nessus Essentials

Chociaż wszystkie systemy komputerowe mają problemy z bezpieczeństwem, wielu ataków można uniknąć dzięki starannej analizie i konserwacji systemu, co może obejmować praktyki od ustanowienia wydajnego, regularnego schematu aktualizacji po przeglądanie plików dziennika pod kątem oznak nietypowej aktywności. Gdy Microsoft dowiaduje się o problemach lub lukach w swoim

oprogramowaniu, publikuje poprawki, aktualizacje zabezpieczeń, pakiety Service Pack i poprawki, aby rozwiązać je tak szybko, jak to możliwe.

Korzystanie z Nessus Essentials

W Ćwiczeniu 8-2 będziesz używać Nessus Essentials na komputerze z systemem Microsoft Windows. Jeśli masz dostęp do serwera Windows, który możesz skanować, użyj go jako celu. Możesz również przeskanować swój własny komputer, aby sprawdzić, jakie luki w zabezpieczeniach może wykryć Nessus Essentials

Aktywność 8-2: Skanowanie komputera lokalnego za pomocą Nessus

Czas trwania: 30 minut

Cel: Skanowanie komputera lokalnego za pomocą Nessus w poszukiwaniu luk w zabezpieczeniach.

Opis: W tej aktywności skanujesz komputer za pomocą Nessus, aby wykryć luki w zabezpieczeniach, w tym słabe lub brakujące hasła. Pod koniec aktywności prześlij instruktorowi podsumowanie swoich ustaleń wraz z krótkimi zaleceniami dotyczącymi rozwiązania znalezionych problemów.

1. Zaloguj się do Nessus Essentials. Na stronie Moje skany kliknij przycisk Nowe skanowanie

2. Na stronie Szablony skanowania wybierz podstawowe skanowanie sieci w sekcji LUKI w zabezpieczeniach.

3. Na karcie Ustawienia na stronie Nowe skanowanie/Podstawowe skanowanie sieci wprowadź nazwę, opis i folder dla skanowania. W polu Cele wprowadź adres IP komputera, który chcesz skanować. Nie musisz podawać danych uwierzytelniających na karcie Dane uwierzytelniające, ale jeśli to zrobisz, skanowanie może zebrać więcej informacji. Kliknij Zapisz.

4. Na stronie Moje skany kliknij przycisk Uruchom, aby rozpocząć nowe skanowanie. Zielona ikona koła wskazuje, że skanowanie jest w toku.

NAJLEPSZE PRAKTYKI DLA SYSTEMÓW WINDOWS

Jako tester penetracyjny Twoim zadaniem jest znajdowanie luk i zgłaszanie ich zgodnie z definicją zawartą w umowie. Twoja odpowiedzialność kończy się na tym. Jednak testerzy bezpieczeństwa muszą nie tylko znajdować luki; muszą znać metody ich korygowania. Zazwyczaj menedżerowie chcą, aby rozwiązania były dołączone do raportów o potencjalnych problemach, szczególnie w przypadku technologii, których mogą nie do końca rozumieć. Chociaż jedynym sposobem na zapewnienie prawdziwego bezpieczeństwa systemu jest odłączenie go od zasilania i zamknięcie w sejfie, takie podejście przeczy celowi sieci. Ponieważ nie można zamknąć komputerów sieciowych, aby zapewnić ich bezpieczeństwo, najlepszą opcją jest zachowanie czujności. Naruszenie bezpieczeństwa jest oddalone tylko o jedną nieodkrytą lukę, ale przy ostrożnym zarządzaniu większość systemów można odpowiednio zabezpieczyć i nadal spełniać potrzeby użytkowników. Ogólne praktyki dotyczące zapewniania i utrzymywania bezpieczeństwa sieci omówiono w poniższych sekcjach.

Łatanie systemów

Najlepszym sposobem na zapewnienie bezpieczeństwa systemów, ich maksymalnej wydajności i korzystania z najnowszych funkcji jest aktualizowanie systemów, nad którymi sprawujesz opiekę. Jak wspomniano, wiele ataków wykorzystuje znaną lukę w zabezpieczeniach, dla której dostępna jest poprawka. Istnieje kilka metod uzyskiwania pakietów serwisowych, poprawek i poprawek. Jeśli masz do utrzymania tylko kilka komputerów (10 lub mniej), dostęp do usługi Windows Update ręcznie z

każdego komputera działa dobrze, ale ta metoda nadal jest czasochłonna. W zależności od wersji systemu Windows możesz skonfigurować automatyczne aktualizacje na każdym komputerze. Ta opcja jest zwykle lepsza, ponieważ pomaga zapewnić, że komputery są zawsze aktualne bez interwencji administratora lub użytkownika. Wadą jest to, że niektóre poprawki mogą powodować problemy, więc lepiej jest przetestować poprawkę przed zastosowaniem jej w systemie produkcyjnym, szczególnie w dużych sieciach. W przypadku dużej sieci ręczne stosowanie aktualizacji nie jest wykonalne. Konfigurowanie automatycznych aktualizacji jest opcją, jeśli masz fizyczny dostęp do wszystkich komputerów, chociaż pobieranie poprawek na każdy komputer może spowolnić działanie sieci. Masz kilka opcji zarządzania poprawkami. W latach 1994–2005 serwer Systems Management Server (SMS) firmy Microsoft był standardem zarządzania poprawkami zabezpieczeń systemu Windows na wielu komputerach w sieci. Ta usługa oceniała maszyny w określonej domenie i mogła zostać skonfigurowana do zarządzania wdrażaniem poprawek. (Chociaż ta usługa miała wiele innych możliwości, na potrzeby tego modułu wystarczy wiedzieć, że może być używana do zarządzania poprawkami.) W 2005 r. udostępniono usługi Windows Software Update Services (WSUS). WSUS to technologia klient/serwer zaprojektowana do zarządzania poprawkami i aktualizacją oprogramowania systemowego z sieci. Zamiast pobierać aktualizacje na każdy komputer, WSUS pobiera poprawki i publikuje je wewnętrznie na serwerach i komputerach stacjonarnych. W przeciwieństwie do funkcji Automatic Updates, która automatycznie pobiera i instaluje aktualizacje, administrator ma kontrolę nad tym, które aktualizacje są wdrażane. Ta funkcja jest dużą zaletą, biorąc pod uwagę, że niektóre aktualizacje mogą powodować problemy z pewnymi konfiguracjami sieci i aplikacji i powinny zostać przetestowane przed wdrożeniem. W 2007 r. Windows System Center Configuration Manager (SCCM) stał się nowym standardem. SCCM obejmuje zestaw narzędzi, które pomagają administratorom wdrażać i zarządzać serwerami wraz z zaktualizowaną funkcjonalnością zarządzania poprawkami. SCCM pozwala nawet administratorom kontrolować urządzenia mobilne z systemem Android, iOS i Windows Mobile OS. Rozwiązania do zarządzania poprawkami innych firm są również dostępne u dostawców, takich jak BigFix, Tanium i BladeLogic. Bez względu na to, jakich narzędzi do zarządzania poprawkami używasz, pamiętaj, że aktualizowanie systemów jest jednym z najważniejszych kroków w utrzymaniu ich bezpieczeństwa. Jako tester bezpieczeństwa często odkryjesz, że poprawki nie są aktualne w testowanym systemie. Skuteczny schemat zarządzania poprawkami może wydawać się zdrowym rozsądkiem, ale administratorzy mogą być tak zajęci innymi skomplikowanymi problemami, że zapominają o prostych rozwiązaniach. Musisz polecić swoim klientom skuteczne zarządzanie poprawkami i być w stanie wyjaśnić, dlaczego jest ono kluczowe dla bezpieczeństwa systemu.

Rozwiązania antywirusowe

Niezależnie od tego, czy pracujesz z siecią przedsiębiorstwa składającą się z tysięcy serwerów i dziesiątek tysięcy klientów, czy z małą siecią biznesową składającą się z 15 systemów i jednego serwera, musisz użyć rozwiązania antywirusowego. W przypadku małych sieci mogą wystarczyć narzędzia antywirusowe na komputery stacjonarne z automatyczną aktualizacją, ale w dużej sieci potrzebne jest rozwiązanie na poziomie korporacyjnym. Dostępnych jest kilka doskonałych produktów, a wybranie właściwego wymaga pewnych badań. Narzędzie antywirusowe musi być zaplanowane, zainstalowane i poprawnie skonfigurowane, aby zapewnić najlepszą ochronę. Narzędzie antywirusowe jest prawie bezużyteczne, jeśli nie jest regularnie aktualizowane. W idealnym przypadku narzędzie antywirusowe powinno automatycznie pobierać i instalować aktualizacje codziennie. Jeśli badanie systemu wykaże, że żadne narzędzie antywirusowe nie jest uruchomione, należy zalecić natychmiastową instalację. Należy również położyć nacisk na jego aktualizowanie w celu zapewnienia najlepszej ochrony.

Regularnie włączaj rejestrowanie i przeglądaj rejestry

Rejestrowanie jest kluczową funkcją monitorowania bezpieczeństwa systemu. Musi być starannie skonfigurowane, aby rejestrować tylko przydatne statystyki, ponieważ zbyt szczegółowe rejestrowanie może łatwo przytłoczyć analityków. Regularnie sprawdzaj dzienniki pod kątem oznak włamań lub innych problemów w sieci. Buduj zapobieganie i wykrywanie, zastanawiając się, co atakujący mogliby zrobić, gdyby naruszyli Twoją sieć. Gdybyś był atakującym i włamał się do sieci, której nie znasz, prawdopodobnie uruchomiłbyś kilka poleceń administracyjnych systemu Windows, aby lepiej zrozumieć sieć. Polecenia takie jak ipconfig /all, netstat -r, net view i gpresult, zwłaszcza gdy są zgrupowane razem, mogą być postrzegane jako podejrzane, biorąc pod uwagę odpowiedni kontekst. Jeśli użytkownik nietechniczny nagle zgłosi żądania administracyjne, może nadszedł czas na dokładniejsze zbadanie sprawy. Skanowanie tysięcy wpisów w dzienniku jest czasochłonne, a pominięcie ważnych wpisów jest prawdopodobne. Narzędzie do monitorowania dzienników jest najlepsze do tego zadania. Dostępnych jest kilka, w zależności od potrzeb sieci i budżetu. Niektóre z tych narzędzi obejmują nawet konfigurowalną automatyzację, która może dać Ci przewagę nad atakującym poprzez automatyzację odpowiedzi (np. wyłączenie karty sieciowej zdalnego systemu), gdy narzędzia wykryją znane złośliwe działania.

Wyłącz nieużywane usługi i filtruj porty

Wyłączanie niepotrzebnych usług i usuwanie niepotrzebnych aplikacji lub skryptów ma sens, ponieważ w przeciwnym razie daje intruzom potencjalny punkt wejścia do sieci. Na przykład, jeśli masz system Windows Server 2016 działający jako serwer plików, nie potrzebujesz usług DNS działających na nim; w ten sposób port 53 TCP/UDP pozostaje otwarty i podatny na ataki. Chodzi o to, aby otworzyć tylko to, co musi być otwarte i zamknąć wszystko inne — znane również jako zmniejszenie powierzchni ataku. (Powierzchnia ataku to ilość kodu, którą system komputerowy udostępnia nieuwierzytelnionym osobom z zewnątrz). Przy mniejszej liczbie ujawnionych usług atakujący ma mniejsze szanse na znalezienie niezałatanej luki w zabezpieczeniach.

Ponadto filtrowanie niepotrzebnych portów może chronić systemy przed atakiem. Niektóre porty często narażone na ataki obejmują:

• FTP (20 i 21 TCP)

• TFTP (69 UDP)

• Telnet (23 TCP)

• DNS (53 TCP/UDP)

• NTP (123 UDP)

• NetBIOS (135 TCP/UDP, 137 i 138 UDP, 139 TCP)

• SMB (445 TCP/UDP)

• Remote Desktop Protocol (3389 TCP)

• SNMP (161 i 162 TCP/UDP)

• Programy Windows RPC (1025 do 1039 TCP/UDP)

Najlepszym sposobem ochrony sieci przed atakami SMB jest upewnienie się, że routery obwodowe i zapory filtrują porty od 137 do 139 i 445. Blokowanie portów 139 i 445 ma dodatkową zaletę w postaci ochrony przed zewnętrznymi atakami sesji zerowych. Windows Server 2003 domyślnie nie wyłącza protokołu SMB na porcie 445. W rzeczywistości, jeśli komputer jest kontrolerem domeny, należy

zapewnić dostęp do protokołu SMB. Zadaniem serwera jest upewnienie się, że osoba próbująca zalogować się do sieci jest rzeczywiście upoważniona do dostępu do zasobów sieciowych. Ponieważ zazwyczaj chcesz udostępniać zasoby na serwerze, zamknięcie portu 445 może spowodować inne problemy, takie jak brak dostępu użytkowników do udostępnionych folderów i drukarek. Atakujący może uzyskać dostęp przez wiele innych portów. Nie można zamknąć wszystkich dróg ataku i nadal oferować użytkownikom potrzebną funkcjonalność, ale dzięki starannemu planowaniu administrator może zmniejszyć liczbę dróg do sieci. Aby uzyskać pełną listę portów i usług, zapoznaj się ze stroną IANA Assigned Port Number na stronie www.iana.org/assignments/port-numbers.

UWAGA: Zachowaj ostrożność podczas wyłączania usług i blokowania portów. Upewnij się, że żadne wymagane usługi zależne od portu lub innej usługi nie zostały przypadkowo wyłączone.

Inne najlepsze praktyki bezpieczeństwa

Oprócz aktualizowania oprogramowania, uruchamiania narzędzi antywirusowych i wyłączania usług, możesz podjąć następujące kroki, aby zminimalizować ryzyko dla sieci Windows:

• Zminimalizuj liczbę użytkowników z uprawnieniami administracyjnymi.

• Wdróż oprogramowanie, aby zapobiec wydostawaniu się poufnych danych z sieci.

• Użyj segmentacji sieci, aby utrudnić atakującemu przechodzenie z komputera na komputer.

• Ogranicz liczbę aplikacji, które mogą być uruchamiane na komputerze podłączonym do sieci.

• Usuń nieużywane skrypty i przykładowe aplikacje.

• Usuń domyślne ukryte udziały i niepotrzebne udziały.

• Użyj innego unikalnego schematu nazewnictwa i haseł dla interfejsów publicznych.

• Upewnij się, że długość i złożoność haseł są wystarczające.

• Uważaj na domyślne uprawnienia, konfiguracje i hasła.

• Użyj technologii filtrowania pakietów, takich jak zapory programowe oparte na hoście, zapory sprzętowe klasy korporacyjnej oraz systemy wykrywania i zapobiegania włamaniom, które są dostosowane do środowiska.

• Użyj narzędzi typu open source lub komercyjnych do oceny bezpieczeństwa systemu.

• Użyj narzędzia do sprawdzania integralności plików, aby monitorować nieautoryzowane modyfikacje systemu plików i wysyłać alerty o tych zmianach.

• Wyłącz konto gościa.

• Wyłącz lokalne konto administratora.

• Wyłącz konta użytkowników, którzy nie są już w firmie.

• Upewnij się, że żadne konto nie ma pustych haseł. Solidna polityka haseł jest kluczowa.

• Użyj zasad grupy systemu Windows, aby skutecznie i spójnie egzekwować konfiguracje zabezpieczeń w dużych sieciach.

• Opracuj kompleksowy program świadomości bezpieczeństwa dla użytkowników, aby wzmocnić politykę bezpieczeństwa swojej organizacji.

• Bądź na bieżąco z pojawiającymi się zagrożeniami. Skontaktuj się z Microsoft, SANS, US-CERT (www.us-cert.gov) i innymi organizacjami ds. bezpieczeństwa, aby uzyskać najnowsze informacje.

Dziedzina bezpieczeństwa zmienia się szybko, a specjaliści ds. bezpieczeństwa muszą nadążać za nowymi rozwiązaniami, zagrożeniami i narzędziami. Zabezpieczanie systemów Windows może być trudne, ale masz dostęp do wielu narzędzi, aby zlokalizować problemy.

LUKI W ZABEZPIECZENIACH SYSTEMU LINUX

Jak każdy system operacyjny, Linux może być bezpieczniejszy, jeśli użytkownicy będą świadomi jego luk w zabezpieczeniach i będą na bieżąco z nowymi wersjami i poprawkami. Zakłada się, że masz pewne doświadczenie w pracy z systemem operacyjnym *nix, więc podstawy systemu operacyjnego Linux i systemu plików nie są omawiane w tym module. Dostępnych jest wiele wersji systemu Linux, różniących się od niewielkich do poważnych. Na przykład Red Hat i Fedora Linux używają polecenia yum do aktualizowania i zarządzania pakietami RPM (Red Hat Package Manager), a Ubuntu, Debian i Kali Linux używają polecenia apt-get do aktualizowania i zarządzania pakietami DEB (Debian). Bez względu na to, jakiej wersji systemu Linux używasz, musisz zrozumieć podstawy, takie jak kontrola uruchamiania i konfiguracja usług, struktura katalogów, system plików, podstawowe polecenia powłoki i skrypty oraz zarządzanie pakietami. (Jeśli nie znasz tych podstaw *nix, poświęć trochę czasu na ich przejrzenie. Jednym z najszybszych sposobów, w jaki testerzy bezpieczeństwa mogą zrobić złe wrażenie na klientach, jest pokazanie braku wiedzy na temat testowanych systemów.) Typowa dystrybucja Linuksa ma tysiące pakietów opracowanych przez wielu współpracowników z całego świata. Przy tak zróżnicowanych źródłach kodu nieuniknione jest, że część kodu będzie miała wady, które czasami są odkrywane dopiero po włączeniu ich do produktu końcowego. Zbyt wielu administratorów sieci uważa, że system Windows jest łatwiejszy do zaatakowania i postrzega systemy operacyjne *nix jako z natury bezpieczniejsze. Specjaliści ds. bezpieczeństwa muszą zrozumieć, że przyjmowanie takich założeń może być niebezpieczne, ponieważ wszystkie systemy operacyjne mają luki w zabezpieczeniach. Podczas przeprowadzania testu bezpieczeństwa w systemach z systemem Linux należy przestrzegać tych samych zasad, których należy przestrzegać w przypadku każdego innego systemu operacyjnego.

Samba

Użytkownicy oczekują współdzielenia zasobów w sieci, niezależnie od używanego systemu operacyjnego, a firmy odkryły, że użytkownicy nie tolerują już zastrzeżonych systemów, które nie mogą współistnieć w sieci. Aby rozwiązać problem interoperacyjności, grupa programistów stworzyła Sambę (www.samba.org) w 1992 r. jako implementację CIFS typu open source. Dzięki Sambie serwery *nix mogą współdzielić zasoby z klientami Windows, a klienci Windows mogą uzyskiwać dostęp do zasobu *nix, nie zdając sobie sprawy, że zasób znajduje się na komputerze *nix. Samba została również przeniesiona na systemy inne niż *nix, w tym OpenVMS, NetWare i AmigaOS. W momencie pisania tego tekstu specjaliści ds. bezpieczeństwa powinni mieć podstawową wiedzę na temat SMB i Samby, ponieważ wiele firm ma mieszane środowisko systemów Windows i *nix. Aby uzyskać dostęp do zasobu *nix z komputera z systemem Windows, CIFS musi być włączony na obu systemach. W sieciach wymagających komputerów *nix dostępu do zasobów Windows często używana jest Samba. Nie jest to narzędzie hakerskie; ten produkt został zaprojektowany, aby umożliwić komputerom *nix „oszukanie" usług Windows, aby uwierzyły, że zasoby *nix są zasobami Windows. Klient *nix może połączyć się z udostępnioną drukarką Windows i odwrotnie, gdy Samba jest skonfigurowana na komputerze *nix. Większość nowych wersji Linuksa zawiera Sambę jako opcjonalny pakiet, więc nie trzeba jej pobierać, instalować i kompilować.

Narzędzia do identyfikacji luk w zabezpieczeniach Linuksa

Odwiedzenie witryny CVE to dobry pierwszy krok w odkrywaniu możliwych ścieżek, którymi atakujący mogą włamać się do systemu Linux. Aby dać ci pojęcie o mnogości luk w zabezpieczeniach Linuksa, znaleziono ponad 500 wpisów. Wiele z tych luk nie może być już wykorzystanych w systemach, które zostały zaktualizowane. Możesz użyć informacji CVE podczas testowania komputerów z systemem Linux pod kątem znanych luk. Testerzy bezpieczeństwa powinni dokładnie przejrzeć informacje CVE i CAN, aby upewnić się, że system nie ma żadnych luk wymienionych na stronie internetowej CVE i został zaktualizowany. Dowiedziałeś się, jak narzędzia takie jak OpenVAS (znane również jako Greenbone Security Assistant) mogą wyliczać wiele systemów operacyjnych. Za pomocą narzędzi wyliczania tester bezpieczeństwa może wykonać następujące czynności:

• Zidentyfikować komputer w sieci za pomocą skanowania portów i transferów stref.

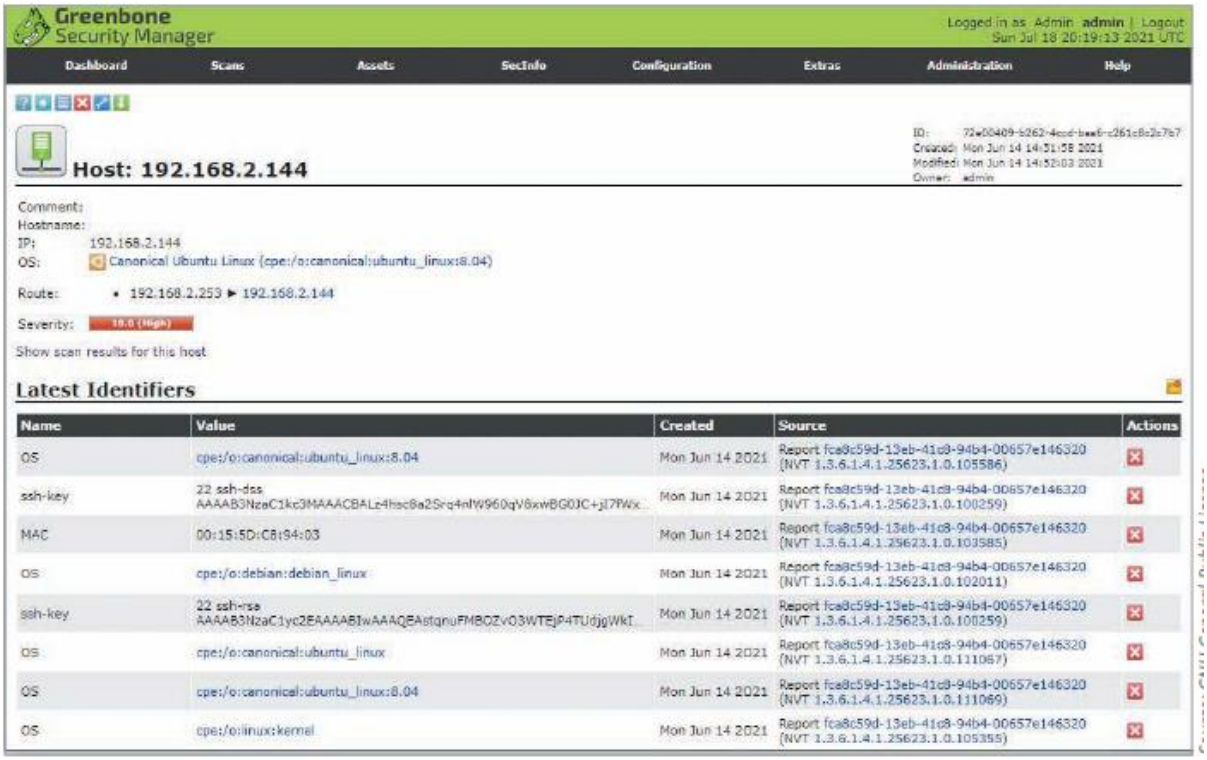
• Zidentyfikować system operacyjny używany przez komputer, przeprowadzając skanowanie portów i wyliczanie.

• Zidentyfikować, za pomocą wyliczania, wszystkie konta logowania i hasła skonfigurowane na komputerze.

• Poznać nazwy folderów współdzielonych za pomocą wyliczania.

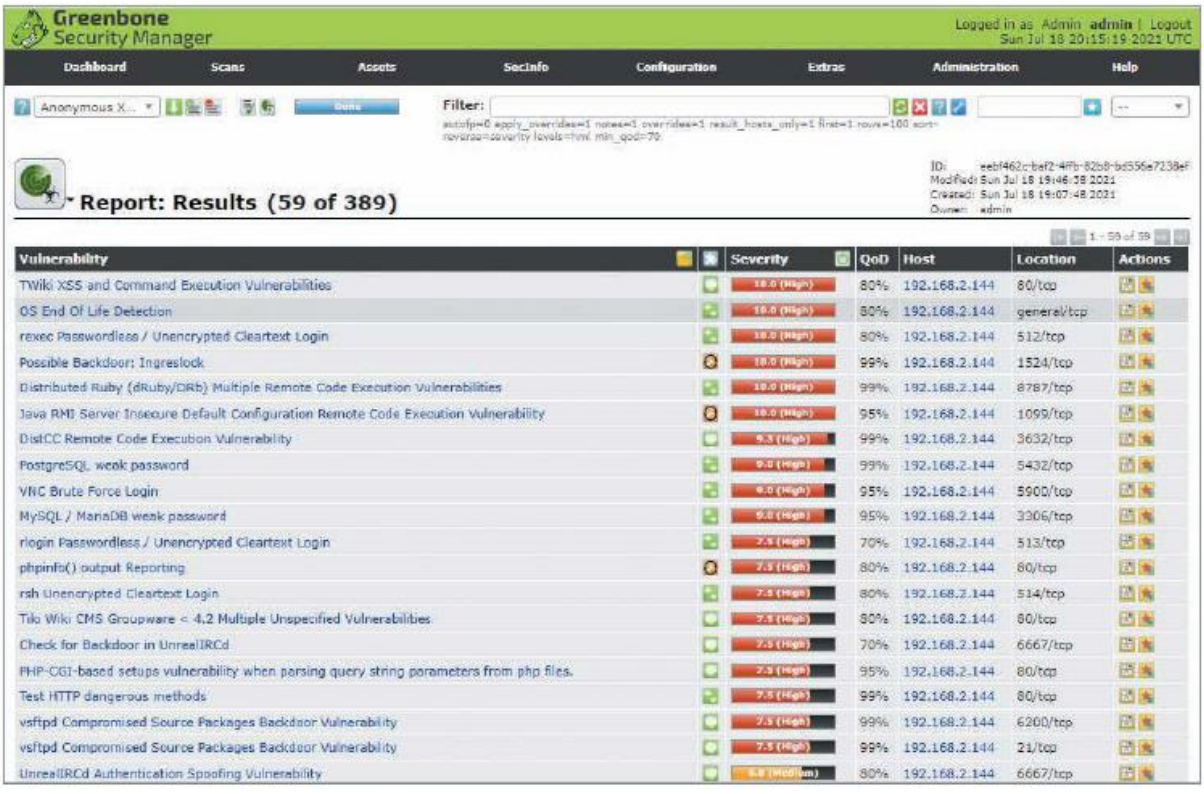
• Zidentyfikować usługi uruchomione na komputerze.

Poniższy przykład pokazuje wyliczanie i znajdowanie luk przez OpenVAS na komputerze z systemem Linux. Rysunek pokazuje raport OpenVAS po przeskanowaniu komputera Linux o adresie IP 192.168.2.144. Rysunek wskazuje, że OpenVAS wykrył system Ubuntu Linux.



Na rysunku zauważ, że OpenVAS odkrył 39 luk wysokiego ryzyka, 73 luki średniego ryzyka i 6 luk niskiego ryzyka. Widać, że ta maszyna nie była łatana od jakiegoś czasu.

Możesz przeglądać poszczególne luki w zabezpieczeniach, klikając opcję Skanowania na pasku nawigacyjnym w celu wyświetlenia strony Wyniki, jak pokazano na rysunku .



Przy 39 lukach wysokiego ryzyka omówienie wyników przedstawionych na Rysunku 8-8 wymagałoby całego modułu, ale można zobaczyć, jak OpenVAS może być używany do testowania bezpieczeństwa. Rysunek pokazuje, że OpenVAS odkrył krytyczną lukę „Possible Backdoor: Ingreslock”.

Backdoor to luka, w której haker może potajemnie połączyć się z otwartym portem na zainfekowanym komputerze i przejąć nad nim kontrolę. Rysunek 8-9 pokazuje 1524/tcp pod nagłówkiem Lokalizacja, co oznacza, że port 1524 jest otwarty. Ingres to baza danych SQL, która jest powszechnie używana do obsługi bardzo dużych komercyjnych aplikacji rządowych. Ingres został zaprojektowany tak, aby mieć otwarty port 1524, chociaż ten port jest często wykorzystywany jako backdoor przez hakerów. Używając netcat z wiersza poleceń lub podobnego narzędzia, atakujący mogą połączyć się z tym portem i rozpocząć swoje nikczemne działania. Jeśli ten system jest serwerem skierowanym do Internetu, ta luka stanowi poważne ryzyko, które mogą wykorzystać zewnętrzni aktorzy. Jeśli ten system nie jest podłączony do Internetu, nadal jest podatny na wewnętrzne zagrożenia sieciowe.

Instalowanie i używanie OpenVAS w celu wykrywania luk w zabezpieczeniach komputera z systemem Linux

Czas trwania: 45 minut

Cel: Zainstaluj i użyj OpenVAS, aby odkryć luki w zabezpieczeniach na komputerze z systemem Linux.

Opis: OpenVAS to przydatne narzędzie do enumeracji systemu operacyjnego. Nie tylko ostrzega testerów o możliwych lukach, ale także zaleca, jak naprawić wykryte problemy. W tej aktywności konfigurujesz OpenVAS, aby przeskanował komputer z systemem Linux Twojego partnera (lub, jeśli pracujesz sam, swój własny komputer z systemem Linux) i odkrył wszelkie luki, których atakujący mógłby użyć, aby uzyskać dostęp.

1. Uruchom system Kali Linux.

2. Otwórz powłokę terminala i określ adres IP swojego komputera, wpisując ifconfig i naciskając Enter. Zapisz adres IP i przekaż go swojemu partnerowi. Następnie uruchom demona ssh (sshd), wpisując /etc/init.d/ssh start i naciskając Enter. To polecenie umożliwia OpenVAS na komputerze Twojego partnera zalogowanie się i sprawdzenie luk w zabezpieczeniach.

3. Wpisz sudo apt-get install openvas, naciśnij Enter, a następnie naciśnij y, gdy pojawi się monit o pobranie i zainstalowanie pakietu Open VAS. Poczekaj, aż ten proces się zakończy.

4. Wpisz sudo gvm-setup i naciśnij Enter, aby rozpocząć proces instalacji OpenVAS, który zajmuje kilka minut. (OpenVAS to składnik skanera Greenbone Vulnerability Manager (GVM), a to, co kiedyś było openvas-setup, teraz jest gvm-setup.) Poczekaj, aż setup wyświetli komunikat „Użytkownik utworzony z hasłem:

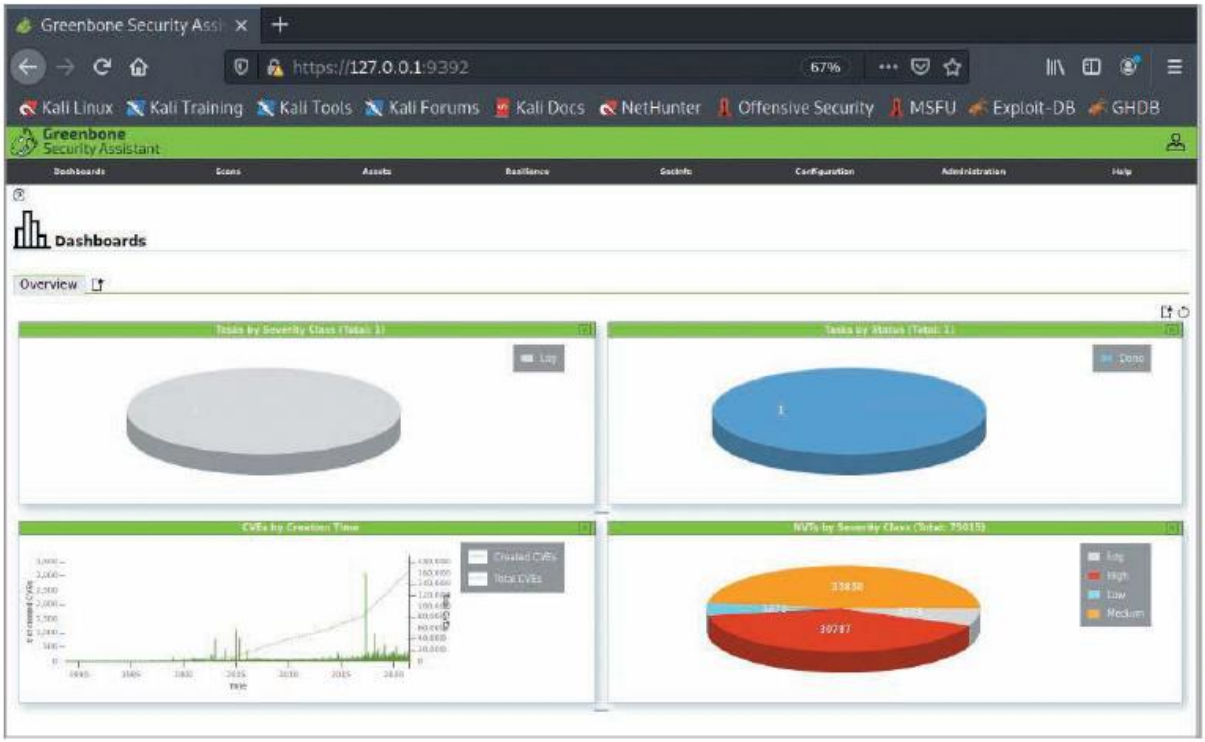
<długi losowy ciąg>". Ten długi losowy ciąg to hasło do konta administratora, więc skopiuj je na później. Jeśli nie widzisz tego komunikatu lub musisz zresetować hasło administratora, użyj polecenia su - _gvm -s /bin/sh -c "gvmd --user=admin --new-password mypasswd; history -c" i naciśnij Enter.

5. Wpisz gvm-check-setup i naciśnij Enter, aby sprawdzić konfigurację. Jeśli polecenie znajdzie problemy, postępuj zgodnie z każdą instrukcją polecenia, aby rozwiązać problem. Kontynuuj uruchamianie polecenia gvm-check-setup, aż zgłosi, że konfiguracja jest prawidłowa.

6. OpenVAS używa kanałów społecznościowych (aktualizacji danych), aby aktualizować swoje bazy danych CVE i NVT (zagrożeń podatności sieci). Wpisz sudo gvm-feed-update i naciśnij Enter, aby połączyć się z kanałami i rozpocząć pobieranie aktualizacji.

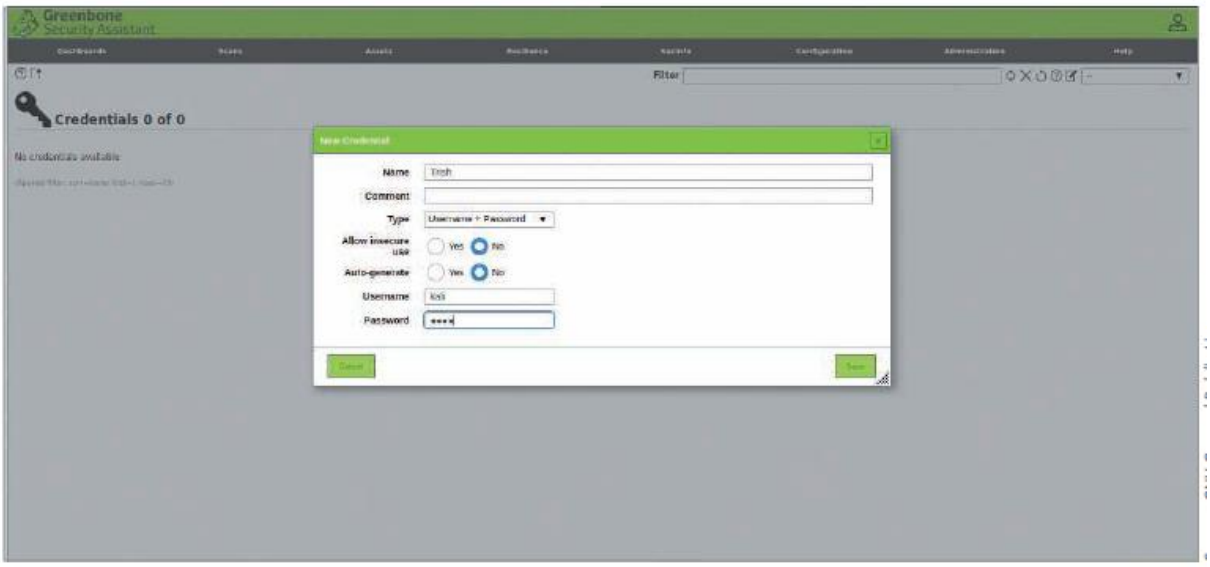
7. Wpisz sudo gvm-start i naciśnij Enter, aby upewnić się, że usługi Open VAS są uruchomione. To polecenie może również automatycznie otworzyć przeglądarkę internetową na stronie logowania OpenVAS.

8. Po zainstalowaniu i uruchomieniu OpenVAS możesz uzyskać do niego dostęp, otwierając przeglądarkę internetową i przechodząc do https://127.0.0.1:9392. Użyj admin jako nazwy użytkownika i długiego losowego ciągu skopiowanego w kroku 4 jako hasła. Krok 4 zawiera również instrukcje resetowania tego hasła. Po uwierzytelnieniu zobaczysz okno podobne do tego, które pokazano na rysunku.

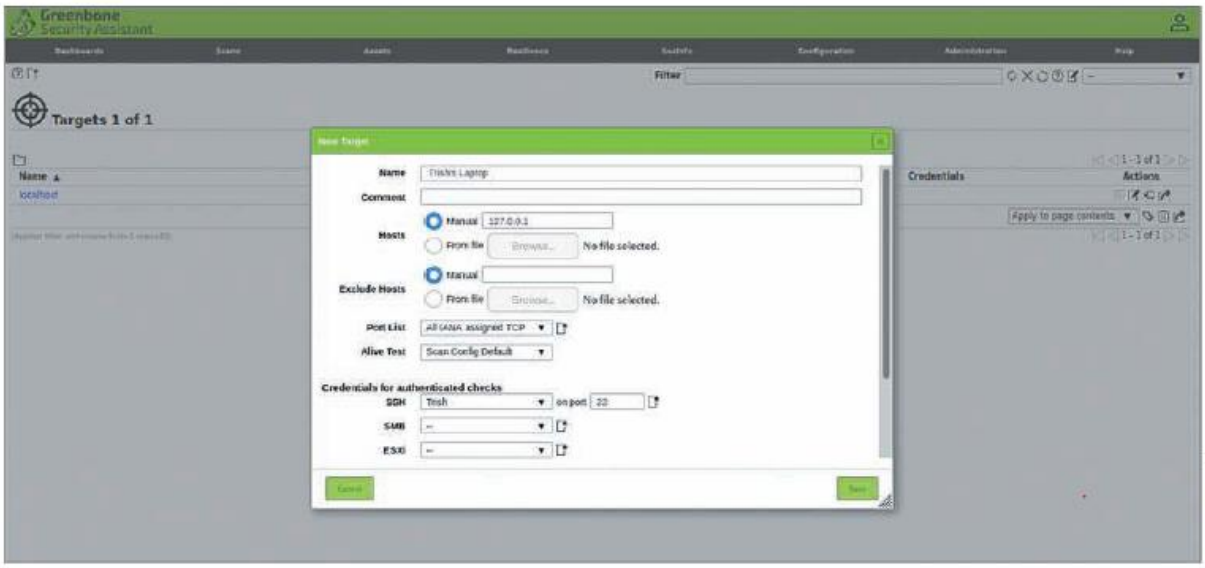


Jeśli wykresy CVE lub NVT wydają się nie pokazywać żadnych danych, być może będziesz musiał poczekać, aż kanały zostaną zaktualizowane lub wypróbować niektóre z kroków rozwiązywania problemów wymienionych w uwadze na końcu tej aktywności.

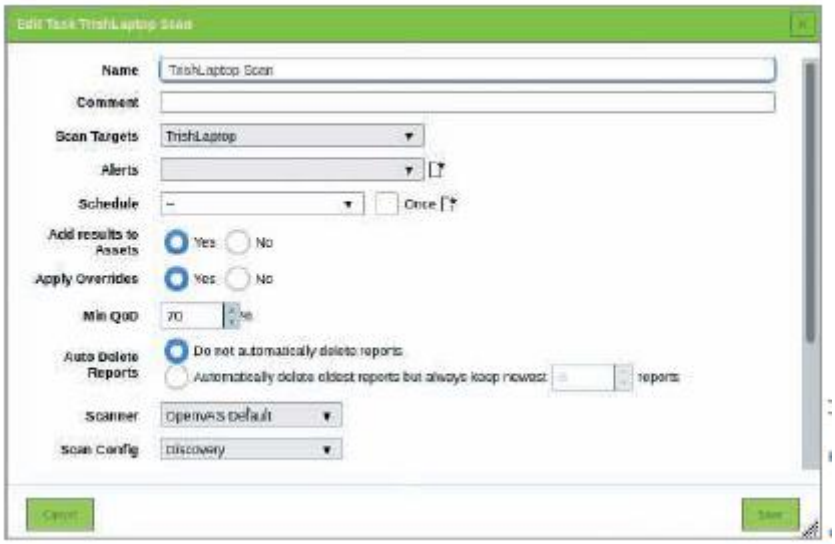
9. Wskaż kartę Konfiguracja i wybierz Poświadczenia z listy rozwijanej. Wybierz różdżkę nad grafiką klucza, aby dodać nowe poświadczenie. Pozwól swojemu partnerowi wprowadzić główne poświadczenie swojego systemu w formularzu Nowe poświadczenie, pokazanym na rysunku. Kliknij Zapisz i pozwól OpenVAS na kilka minut na przetworzenie tego żądania.



10. Wskaż kartę Konfiguracja i wybierz Cele z listy rozwijanej. Wybierz jasnoniebieską ikonę z białą gwiazdką, aby dodać nowy cel. Wypełnij formularz Nowy cel informacjami o systemie swojego partnera. Nazwij komputer partnera zadania (zastępując partner nazwą swojego partnera). Upewnij się, że wybrałeś skonfigurowane poświadczenie SSH, podobnie jak na rysunku .



11. Wskaż kartę Scan Management i wybierz zadania z menu rozwijanego. Obok „Tasks (total: 0)” wybierz jasnoniebieską ikonę z białą gwiazdką, aby dodać nowe zadanie skanowania. Nazwij zadanie partnera scan (zastępując partner nazwą partnera). Wybierz komputer partnera z listy rozwijanej Scan Targets, a następnie kliknij create task. Szczegóły zadania powinny wyglądać podobnie do rysunku.



12. Teraz, gdy wszystko jest skonfigurowane, uruchom skanowanie ze strony Skanowanie, klikając przycisk Odtwórz (czarno-biały trójkąt skierowany w prawo). Poczekaj na zakończenie skanowania. Możesz nie znaleźć wielu luk, jeśli system docelowy jest aktualny.

13. Po zakończeniu skanowania wyświetl wyniki, klikając 1 obok Raporty. Aby dowiedzieć się więcej, kliknij datę i godzinę skanowania.

14. Korzystając z informacji odkrytych przez OpenVAS, zapisz najpoważniejszą lukę w zabezpieczeniach docelowego systemu i wyjaśnij, dlaczego jest krytyczna. Dołącz identyfikator odniesienia CVE. Jakie zalecenia dotyczące naprawy tej luki w zabezpieczeniach przedstawia OpenVAS?

15. Aby zamknąć OpenVAS, zamknij okno. Gdy pojawi się monit o zapisanie raportu, kliknij Nie, a następnie kliknij Zakończ w oknie dialogowym Konfiguracja OpenVAS. Pozostaw system Linux uruchomiony do następnej czynności.

UWAGA

Aby mieć pewność, że Twoje kanały danych OpenVAS CVE i NVT są aktualizowane, możesz wybrać CVE lub NVT z menu OpenVAS SecInfo. Jeśli którykolwiek z nich nie pokazuje danych, wypróbuj następujące kroki:

1. Wyjdź z interfejsu OpenVAS/GVM, zamykając przeglądarkę.

2. Otwórz powłokę terminala, wprowadź polecenie gvm-stop, a następnie naciśnij Enter.

3. Wpisz sudo runuser -u _gvm -- greenbone-nvt-sync --rsync i naciśnij Enter. To polecenie próbuje zsynchronizować/zaktualizować bazę danych NVT. (Zajmuje to kilka minut).

4. Wpisz sudo greenbone-scapdata-sync i naciśnij Enter. To polecenie próbuje zsynchronizować/zaktualizować bazę danych SCAP. (Zajmuje to kilka minut).

5. Wpisz sudo greenbone-certdata-sync i naciśnij Enter. To polecenie próbuje zsynchronizować/zaktualizować bazę danych CERT. (Zajmuje to kilka minut.)

6. Uruchom ponownie Kali Linux, wpisując sudo reboot i naciskając Enter.

7. Zaloguj się ponownie do Kali Linux i w powłoce terminala wpisz gvm-start i naciśnij Enter.

Po odkryciu luki atakujący mogą przejść do witryny opisującej exploity wykorzystujące lukę. W Ćwiczeniu odwiedzasz inną witrynę z informacjami o exploitach, a także wieloma artykułami i narzędziami dla testerów bezpieczeństwa.

UWAGA

Niektóre pakiety oprogramowania w instalacji Kali mogą nie być najnowszymi wersjami. Nawet po kilku miesiącach bez zainstalowanych poprawek system Linux może stać się kopalnią luk dla atakującego. Tester bezpieczeństwa prawdopodobnie zaleciłby uaktualnienie wersji przed poświęceniem czasu na poszukiwanie luk. Możesz użyć polecenia apt-get update && upgrade, aby zaktualizować system Kali Linux o najnowsze poprawki.

Odkrywanie exploitów dla systemów Linux

Czas trwania: 20 minut

Cel: Przeszukaj Internet, aby odkryć exploity dla systemu Linux.

Opis: W tej aktywności odwiedzasz witrynę internetową, która zawiera listę exploitów, których możesz użyć do atakowania różnych systemów operacyjnych. Jako tester bezpieczeństwa powinieneś znać zasoby dostępne zarówno dla testerów bezpieczeństwa, jak i atakujących.

1. W razie potrzeby uruchom komputer w systemie Kali Linux. Uruchom przeglądarkę internetową i przejdź do witryny www.exploit-db.com.

2. Na stronie EXPLOITS kliknij przycisk Filters (Filtry) i wybierz opcję Linux z listy rozwijanej Platforma. (Jeśli nie jesteś na stronie EXPLOITS (EKSPLOITY), kliknij ikonę błędu w panelu nawigacyjnym po lewej stronie). Wybranie opcji Linux filtruje listę, aby wyświetlić tylko exploity dla systemu Linux. W polu wyszukiwania wpisz wget. To jeszcze bardziej zawęża listę, aby wyświetlić exploity obejmujące polecenie wget Linux.

3. W kolumnie Tytuł kliknij hiperłącze „GNU wget<1.18 – Arbitrary File Upload/ Remote Code Execution” z dnia 2016-07-06.

4. Przeczytaj informacje na stronie o tym exploicie. Opisuje on lukę i zawiera kod Pythona, który może zostać użyty do wykorzystania tej luki. (Przewiń w dół, aby wyświetlić kod Pythona.)

5. Na górze strony kliknij hiperłącze 2016-4971 pod nagłówkiem CVE:, aby wyświetlić National Vulnerability Database, w którym możesz przeczytać oficjalne informacje o luce.

6. Aby ustalić wersję wget zainstalowaną w środowisku Kali Linux, otwórz powłokę terminala, a następnie wpisz wget -v i naciśnij Enter.

7. Jaka wersja wget jest zainstalowana w Twoim systemie?

8. Czy znaleziony exploit wget zadziałałby w Twoim systemie?

9. Przeglądaj exploit-db.com w poszukiwaniu innych luk w zabezpieczeniach Linuksa.

Sprawdzanie trojanów

Jedną z metod zdalnego atakowania sieci jest instalowanie programów trojańskich, które rejestrują naciśnięcia klawiszy i inne procesy bez wiedzy użytkowników. Trojany mogą zostać zainstalowane po kliknięciu przez użytkownika załącznika do wiadomości e-mail lub podczas pobierania pliku z Internetu,

myśląc, że jest to poprawka lub poprawka bezpieczeństwa dla systemu operacyjnego, którego używają. Ponieważ serwer WWW rejestruje adresy IP wszystkich odwiedzających, gdy użytkownicy pobierają plik z Internetu, atakujący znają adres IP osoby, która pobrała trojana. Po zainstalowaniu na komputerze trojan może wykonywać wiele działań. Czasami reklamuje wyliczone informacje o ofierze na określonym porcie, więc atakujący musi monitorować ten port lub połączyć się z nim, aby zebrać informacje. Innym razem trojan może zostać zaprogramowany tak, aby automatycznie łączyć się z maszyną atakującego. Większość trojanów wykonuje jedną lub więcej z następujących funkcji:

• Umożliwia zdalne administrowanie atakowanym systemem

• Tworzy ukryty serwer plików na atakowanym komputerze, aby pliki mogły być przesyłane i pobierane bez wiedzy użytkownika

• Kradnie hasła i wylicza zainstalowane oprogramowanie z atakowanego systemu i wysyła je do atakującego

• Rejestruje wszystkie naciśnięcia klawiszy, które użytkownik wpisuje, i wysyła wyniki e-mailem do atakującego lub przechowuje je w ukrytym pliku, do którego atakujący może uzyskać zdalny dostęp

• Szyfruje wszystkie pliki użytkownika i żąda za nie okupu

• Niszczy wszystkie dane w systemie ofiary

Programy trojańskie Linux są czasami maskowane jako legalne programy, takie jak df lub tar, ale zawierają kod programu, który może wyczyścić systemy plików na komputerze z systemem Linux lub umożliwić zdalną administrację. Trojany są obecnie trudniejsze do wykrycia, ponieważ programiści opracowują je w celu wykonywania legalnych połączeń na portach wychodzących, których IDS lub zapora normalnie nie wykryłyby. Ponieważ generowany ruch wygląda jak normalny ruch sieciowy, trojana trudno wykryć. Na przykład trojan o nazwie Harry wysyła żądania HTTPS POST przez port 443. Te żądania nie są niczym niezwykłym w sieci. Serwer WWW można następnie skonfigurować tak, aby wydawał polecenia wykonywane na komputerze z systemem Linux. Ruch HTTPS wydaje się być normalnym ruchem sieciowym, ale polecenia wysyłane z serwera WWW mogą zawierać inne polecenia żądające, aby zaatakowany komputer pobrał lub skopiował poufne pliki na zdalny serwer WWW. Niektóre ostatnie trojany są kontrolowane przez zakodowane lub nawet zaszyfrowane polecenia, które atakujący publikują w serwisach społecznościowych. Dla kogoś monitorującego ruch sieciowy pochodzący z tych zainfekowanych systemów aktywność ta może wyglądać jak normalny użytkownik przeglądający Facebooka lub Twittera. Ochrona komputerów z systemem Linux przed trojanami, które specjaliści IT już zidentyfikowali, jest łatwiejsza. Na przykład trojan Linux.Backdoor.Kaiten loguje się automatycznie do witryny Internet Relay Chat (IRC) i czeka na polecenia od atakującego (kontrolera). Oprogramowanie antywirusowe dla systemu Linux od McAfee, Sophos i Symantec może wykryć tego trojana typu backdoor. Jeszcze bardziej niebezpieczne są rootkity zawierające programy binarne trojańskie gotowe do zainstalowania przez intruza, który uzyskał dostęp do roota w systemie. Atakujący mogą wtedy ukryć narzędzia, których używają do przeprowadzania dalszych ataków na system i uzyskać dostęp do programów typu backdoor. Typowym rootkitem Linux jest Linux Rootkit 5 (LRK5), ale programiści malware tworzą inne rootkity niemal codziennie. Gdy rootkit jest instalowany, prawidłowe polecenia są zastępowane programami trojańskimi. Na przykład, jeśli rootkit LRK5 jest zainstalowany na komputerze z systemem Linux, wprowadzenie polecenia Trojan killall pozwala procesom atakującego na kontynuowanie działania, nawet jeśli administrator systemu Linux uważa, że wszystkie procesy zostały zabite. Polecenie ls nie pokazuje plików używanych przez atakującego, a polecenie netstat nie pokazuje podejrzanych połączeń sieciowych, które atakujący tworzy. Więc

wszystko wygląda normalnie dla administratorów systemu Linux, nawet jeśli używają poleceń trojańskich.

Korzystanie z narzędzi do znajdowania rootkitów Linuksa

Czas trwania: 15 minut

Cel: Nauczenie się, jak znajdować rootkity Linuksa w Internecie i korzystanie z programu sprawdzającego rootkity.

Opis: Atakujący mogą łatwo zlokalizować rootkity dla wielu platform Linuksa. W tym ćwiczeniu odwiedzasz witrynę www.packetstormsecurity.org, która zawiera tysiące narzędzi i exploitów, z których mogą korzystać atakujący lub specjaliści ds. bezpieczeństwa. Uruchamiasz również program do wykrywania rootkitów dołączony do Kali Linux, aby znaleźć rootkity działające w Twoim systemie.

1. W razie potrzeby uruchom komputer w systemie Linux, uruchom przeglądarkę internetową i przejdź do witryny www.packetstormsecurity.org.

2. Na stronie głównej kliknij Szukaj na pasku nawigacyjnym, wpisz LRK5, a następnie naciśnij Enter. Wyniki zawierają archiwa plików zawierające przykłady kodu, które demonstrują exploit LRK5.

3. Przejrzyj listę Linux Rootkit 5. Opis zawiera kilka poleceń Linux, które są przechwytywane przez trojana podczas korzystania z tego rootkita. Wymień pięć z tych poleceń.

4. IBM oferuje również bezpłatną usługę o nazwie IBM X-Force Exchange, jednak aby z niej korzystać, trzeba się zarejestrować. IBM X-Force Exchange to platforma wywiadowcza, na której można wyszukiwać i udostępniać informacje dotyczące zagrożeń cyberbezpieczeństwa. Przejdź do https://exchange.xforce.ibmcloud.com/, aby się zarejestrować, a następnie wyszukaj słowa kluczowe lojax. Lojax to kolejny rootkit z konkretnym roszczeniem do sławy. Co w Lojaxie czyni go wyjątkowym?

5. Otwórz powłokę terminala, a następnie wpisz chkrootkit i naciśnij Enter, aby sprawdzić, czy w systemie nie ma rootkitów. Czy rozpoznajesz którekolwiek z poleceń Linux, które zapisałeś w kroku 3?

6. Wyloguj się z sesji Linux, ale pozostaw komputer uruchomiony na potrzeby projektów przypadków na końcu modułu.

UWAGA

Jako tester zabezpieczeń powinieneś okresowo sprawdzać systemy Linux pod kątem zainstalowanych rootkitów.

Więcej środków zaradczych przeciwko atakom na Linuksa

Dowiedziałeś się o niektórych sposobach obrony przed lukami w zabezpieczeniach Linuksa, a w tej sekcji poznasz dodatkowe środki zaradcze chroniące system Linux, zwłaszcza przed atakami zdalnymi. Najważniejszymi zadaniami są szkolenie użytkowników, śledzenie wydań jądra i aktualizacji zabezpieczeń oraz konfigurowanie systemów w celu poprawy bezpieczeństwa. Zapanowanie nad tymi zadaniami jest niezbędnym początkiem ochrony każdej sieci.

Szkolenie w zakresie świadomości użytkowników

Najlepszym sposobem na rozpoczęcie ochrony systemów Linux przed atakami zdalnymi jest utrudnienie inżynierom społecznym uzyskiwania informacji od pracowników. Szkolenie w zakresie świadomości użytkowników powinno obejmować wszystkich pracowników, od personelu biurowego po dyrektora generalnego. Powiedz użytkownikom, że żadnych informacji nie należy przekazywać

osobom trzecim, bez względu na to, jak nieszkodliwe mogą się wydawać. Poinformuj ich, że jeśli atakujący wiedzą, jaki system operacyjny jest używany w firmie, mogą wykorzystać te informacje do przeprowadzania ataków sieciowych. Uświadom użytkowników, że wiele exploitów można pobrać ze stron internetowych i podkreśl, że wiedza o tym, jaki system operacyjny jest uruchomiony, ułatwia atakującym wybór exploita. Naucz użytkowników, aby byli podejrzliwi wobec osób zadających pytania o systemy, których używają, i aby sprawdzali, czy rozmawiają z kimś, kto podaje się za pracownika działu IT. Prośba o numer telefonu, pod który można oddzwonić, to dobry sposób na upewnienie się, że dana osoba pracuje w tej samej firmie. 30-minutowa sesja szkoleniowa dotycząca procedur bezpieczeństwa może ostrzec użytkowników, jak łatwo osoby z zewnątrz mogą naruszyć bezpieczeństwo systemów i uzyskać informacje zastrzeżone.

Aktualizacja

Dostawcy oprogramowania toczą niekończącą się walkę o usuwanie luk w zabezpieczeniach, które odkrywają atakujący. Gdy tylko błąd lub luka w zabezpieczeniach zostanie odkryta i opublikowana w Internecie, dostawcy systemów operacyjnych zazwyczaj powiadamiają klientów o aktualizacjach lub poprawkach. Szybkie instalowanie tych poprawek jest niezbędne do ochrony systemu. Większość dystrybucji Linuksa wyświetla teraz ostrzeżenia, aby poinformować użytkowników, że korzystają ze starych wersji. Ostrzeżenia w najnowszych wersjach Fedory i Ubuntu Linux są trudne do zignorowania. Rysunek przedstawia ostrzeżenie wyświetlane, gdy użytkownik loguje się do systemu Ubuntu 20 Linux, który nie jest aktualny.

Bezpieczna konfiguracja

Do skonfigurowania systemu Linux można użyć wielu metod i narzędzi, aby zapobiec włamaniom. Skanery podatności nie tylko wykrywają brakujące poprawki, ale także pomagają zidentyfikować, kiedy system jest źle skonfigurowany. Powinieneś również używać wbudowanych narzędzi Linux. Security Enhanced Linux (SELinux), projekt Narodowej Agencji Bezpieczeństwa (NSA), jest teraz wbudowany w wiele głównych dystrybucji Linuxa. SELinux zawiera kilka funkcji i modułów, które wykorzystują Mandatory Access Control (MAC), mechanizm bezpieczeństwa systemu operacyjnego, który wymusza reguły dostępu na podstawie uprawnień do interakcji między procesami, plikami i użytkownikami. Jeśli włamanie nastąpi w systemie z systemem SELinux, jest mniej prawdopodobne, że intruz będzie w stanie przejąć pełną kontrolę nad systemem. Zajęcia od dostawców korporacyjnych Linuksa obejmują korzystanie z tego narzędzia, a więcej informacji można znaleźć na stronie https://en.wikipedia.org/wiki/Security-nhanced_Linux lub wyszukując SELinux na dowolnej stronie internetowej dystrybucji Linuksa. Jednym z najlepszych sposobów na obiektywne zmierzenie i raportowanie zabezpieczeń systemu operacyjnego jest użycie bezpłatnych plików PDF z testami porównawczymi i narzędzi udostępnianych przez Center for Internet Security (CIS, www.cisecurity.org/cybersecurity-tools/). Testy te są dostępne dla wielu wersji *nix i Windows. Gdy poświęcisz czas na zabezpieczenie systemu operacyjnego Linux, postępując zgodnie z zaleceniami w

teście porównawczym CIS, Twoja wiedza na temat zabezpieczeń systemu Linux i systemu Linux w ogóle się poprawi. Wreszcie narzędzie Forcepoint do blokowania systemu operacyjnego, wcześniej znane jako Security Blanket, jest teraz projektem typu open source o nazwie „OS Lockdown". OS Lockdown służy do wzmacniania systemów poprzez dostosowywanie ustawień do opublikowanych STIG (Security Technical Implementation Guides), niestandardowych profili utworzonych na podstawie STIG lub od podstaw. OS Lockdown umożliwia audyt systemów pod kątem odchyleń od tych profili. Jako narzędzie typu open source, OS Lockdown jest bezpłatny w użyciu. Możesz zainstalować OS Lockdown w systemach Red Hat, CentOS lub Solaris *nix, aby wzmocnić konfigurację zabezpieczeń systemu za pomocą szablonów. Jeśli Twój klient musi przestrzegać pewnych zasad bezpieczeństwa, OS Lockdown może szybko zabezpieczyć systemy i oszczędzić administratorom systemów *nix godzin ręcznej konfiguracji. OS Lockdown można opisać jako *nixowy odpowiednik korzystania z zasad grupy Windows.

PODSUMOWANIE MODUŁU

• Świeże instalacje systemów operacyjnych Windows, których domyślne ustawienia nie zostały zmienione, stanowią poważne luki w zabezpieczeniach, które atakujący mogą wykorzystać. Witryna CVE jest dobrym miejscem do rozpoczęcia sprawdzania luk w zabezpieczeniach systemu Windows.

• Luki w zabezpieczeniach systemów plików Windows obejmują brak obsługi ACL w FAT i ryzyko złośliwych ADS w NTFS.

• Inne luki w zabezpieczeniach systemu Windows obejmują RPC, mechanizm komunikacji międzyprocesowej, który umożliwia programowi działającemu na jednym hoście uruchamianie kodu na zdalnym hoście; NetBIOS, który jest nadal używany do zapewnienia wstecznej kompatybilności; i SMB, który jest również nadal używany do zapewnienia wstecznej kompatybilności i zawiera lukę w zabezpieczeniach, która umożliwia atakującym przechwytywanie ruchu SMB i zbieranie nazw użytkowników i skrótów haseł.

• W systemie Windows sesje zerowe i domyślne instalacje mogą pozostawiać hasła puste, a zasoby niezabezpieczone, co powoduje poważne problemy.

• Nie tylko systemy operacyjne mogą mieć luki w zabezpieczeniach, które można wykorzystać, ale również aplikacje mogą być podatne na ataki. Na przykład starsze wersje programu Microsoft SQL Server mają krytyczną lukę w zabezpieczeniach SQL zwaną pustym hasłem SA, która umożliwia użytkownikom zdalnym uzyskanie dostępu administratora systemu (SA) za pośrednictwem konta SA na serwerze.

• Ataki przepełnienia bufora mogą umożliwić atakującym uruchomienie dowolnego kodu.

• Użytkownicy stanowią poważną lukę w zabezpieczeniach, dlatego niezbędne jest stworzenie kompleksowej polityki haseł i posiadanie programów szkoleniowych w zakresie świadomości użytkowników.

• Dostępnych jest wiele narzędzi do wykrywania luk w zabezpieczeniach systemów Windows, takich jak Nessus. Niezbędna jest nauka korzystania z więcej niż jednego narzędzia.

• Kroki, które możesz zalecić w celu zabezpieczenia systemów, obejmują aktualizowanie systemów najnowszymi poprawkami i aktualizacjami, uruchamianie narzędzi antywirusowych, włączanie rejestrowania i regularnego przeglądania dzienników, wyłączanie nieużywanych lub niepotrzebnych usług oraz filtrowanie niepotrzebnych portów.

• Luki w zabezpieczeniach systemu operacyjnego Linux można wykryć za pomocą narzędzi bezpieczeństwa, takich jak OpenVAS, oraz na stronie internetowej CVE.

• Aby rozwiązać problem interoperacyjności, grupa programistów stworzyła Sambę jako implementację CIFS typu open source.

• Narzędzia takie jak chkrootkit mogą wykrywać rootkity zainstalowane w systemach Linux.

• Wbudowane narzędzia Linux, takie jak SELinux, są dostępne do bezpiecznej konfiguracji systemów. Ponadto bezpłatne narzędzia testowe są dostępne w Centrum Bezpieczeństwa Internetu, a komercyjne narzędzia z szablonami mogą być używane do szybkiego i łatwego zaostrzania konfiguracji zabezpieczeń.