PROJEKT KOŃCOWY HACKINGU ETYCZNEGO

Witamy w projekcie końcowym Hands-On Ethical Hacking, znanym również jako Grand Unifying Project (GRUP). GRUP składa się z serii działań, które wykonasz, aby zapisać wyniki w dokumencie raportu testów penetracyjnych. W działaniach GRUP będziesz testować podatności, używając niektórych narzędzi omówionych w innych modułach. Wykonasz te testy, używając laboratorium testów penetracyjnych komputerów wirtualnych, które utworzysz. Reszta tego modułu wykona następujące czynności:

1. Poprowadzi Cię przez proces konfigurowania laboratorium testów penetracyjnych.

2. Poprowadzi Cię w tworzeniu szablonu dokumentu raportu testów penetracyjnych, aby zapisać podatności i informacje odkryte podczas testów penetracyjnych.

3. Przydzieli Ci różne działania, używając różnych narzędzi, aby wykonać testy penetracyjne i zebrać informacje do uwzględnienia w raporcie.

KONFIGUROWANIE LABPRATORIUM TESTÓW PENETRACYJNYCH

Laboratorium testów penetracyjnych będzie składać się z szeregu maszyn wirtualnych (VM) działających w Oracle VirtualBox. Zainstalowałeś VirtualBox w Aktywności 2-2. Podłączysz nowe maszyny wirtualne za pomocą sieci adaptera host-only w VirtualBox, tak aby środowisko testowe było odizolowane od innych urządzeń w dowolnej rzeczywistej sieci, do której jesteś podłączony. Użyjesz następujących maszyn wirtualnych:

1. Serwer poczty Axigen: Użyj serwera poczty Axigen zainstalowanego wcześniej.

2. Kali Linux Oracle Virtual Appliance (OVA). Możliwe, że używałeś innej instalacji Kali Linux do poprzednich aktywności w tej książce (takich jak Kali Live USB boot), ale w laboratorium testowym używasz aktualnego Kali OVA. Kali-Linux-2021.2 to wersja używana w tym module. Podczas wykonywania tych laboratoriów pobierz i zainstaluj najnowszą wersję.

3. Metasploitable2 OVA. Metasploitable2 to maszyna wirtualna, która została celowo skonstruowana tak, aby była podatna na ataki. Metasploitable2 został stworzony, aby zapewnić testerom penetracyjnym (pen-testerom) cel zawierający luki w zabezpieczeniach, które mogą być wykorzystane do ćwiczenia testów penetracyjnych (pen-testing).

Komputer, którego używasz do hostowania środowiska laboratoryjnego, potrzebuje co najmniej 8 GB pamięci.

Konfigurowanie VirtualBox

VirtualBox i Axigen Mail Server zostały zainstalowane wcześniej. Jeśli nie masz już zainstalowanych VirtualBox i Axigen, wróć do Aktywności 2-2 i postępuj zgodnie z instrukcjami. Jeśli na komputerze działa wirtualizacja Microsoft Hyper-V, musisz wyłączyć usługę Hyper-V, aby VirtualBox mógł działać. Uruchom polecenie PowerShell bcdedit/set hypervisorlaunchtype off (jako administrator), a następnie uruchom ponownie komputer, aby wyłączyć Hyper-V. VirtualBox będzie hostować zbiór maszyn wirtualnych laboratorium, które będą służyć jako cele testów penetracyjnych. VirtualBox zapewnia opcję sieciową, która umożliwia maszynom wirtualnym komunikację ze wszystkimi urządzeniami w sieci. Jednak w tym module nie chcesz skanować wszystkiego w sieci, ponieważ może to prowadzić do mylących wyników lub dostępu do urządzeń, do których skanowania nie masz uprawnień. Jeśli pracujesz w sieci domowej, możesz zmienić sieć na adapter mostkowy, jeśli chcesz uwzględnić urządzenia domowe w swoich działaniach związanych z testami penetracyjnymi. Inna opcja sieciowa,

zwana siecią wewnętrzną, umożliwia maszynom wirtualnym łączenie się ze sobą, ale nie z hostem. Sieć wewnętrzna nie jest odpowiednia dla tego modułu, ponieważ będziesz używać Nessusa na komputerze hosta do skanowania maszyn wirtualnych, więc potrzebujesz połączenia między komputerem hosta a maszynami wirtualnymi. Dla każdej maszyny wirtualnej w VirtualBox, która jest częścią środowiska laboratoryjnego, musisz zmienić ustawienia sieciowe i połączyć maszynę wirtualną z siecią adaptera tylko-hosta. Aby zmienić ustawienia sieciowe maszyny wirtualnej:

1. W prawym panelu VirtualBox kliknij prawym przyciskiem myszy maszynę wirtualną.

2. Kliknij Ustawienia w menu skrótów.

3. W lewym panelu okna Ustawienia kliknij Sieć.

4. W formularzu Sieć kliknij przycisk Podłączono do, a następnie kliknij Adapter tylko-hosta.

5. Kliknij przycisk Nazwa, a następnie kliknij nazwę sieci adaptera tylko-hosta, na przykład VirtualBox Host-Only Ethernet Adapter

UWAGA: Później w tym module wykonasz skanowanie Nessus różnych celów. Jeśli skanowanie Nessus celu Metasploitable wykryje tylko kilka luk, a nie dziesiątki, możesz spróbować użyć ustawienia Bridged Adapter zamiast Host-only dla wszystkich swoich maszyn wirtualnych i ponownie uruchomić skanowanie.

Konfigurowanie Axigen

Zainstalowałeś serwer poczty Axigen w Aktywności 2-2. Jeśli nie masz już zainstalowanego Axigen, wróć do Aktywności 2-2 i postępuj zgodnie z instrukcjami. Zmień ustawienia sieciowe Axigen, aby łączył się z siecią adaptera hosta.

Instalowanie i konfigurowanie Kali Linux OVA

Być może używałeś innej metody uruchamiania Kali Linux w poprzednich aktywnościach w tym kursie, takiej jak używanie rozruchowego USB na żywo lub pełnej instalacji Linuksa na komputerze, ale w tym module instancja Kali Linux musi znajdować się w VirtualBox. Jeśli masz już zainstalowany Kali Linux w VirtualBox, możesz użyć istniejącej maszyny wirtualnej, o ile zmienisz jej ustawienia sieciowe, aby połączyć ją z siecią adaptera hosta. OVA to skrót od Oracle Virtual Appliance. Urządzenie wirtualne to maszyna wirtualna, która została już zainstalowana na sprzęcie wirtualnym. Importowanie OVA jest wygodniejsze niż budowanie maszyny wirtualnej od podstaw. Aby zainstalować Kali Linux OVA:

1. Użyj przeglądarki, aby przejść do www.kali.org/get-kali/#kali-virtual-machines, a następnie pobierz plik OVA. Wybierz wersję VirtualBox 64-bit.

2. W VirtualBox kliknij Plik na pasku menu, a następnie kliknij Importuj urządzenie.

3. W oknie dialogowym Importuj urządzenie wirtualne kliknij ikonę folderu, aby przejść do pliku OVA, który wcześniej pobrałeś, i wybrać go

4. Po wybraniu pliku OVA kliknij Dalej.

5. Przejrzyj ustawienia urządzenia, a następnie kliknij Importuj, aby rozpocząć importowanie.

6. Gdy otworzy się okno Umowa licencyjna oprogramowania, kliknij Zgadzam się, aby kontynuować.

7. Po zakończeniu importowania kliknij prawym przyciskiem myszy maszynę wirtualną Kali, kliknij Ustawienia w menu skrótów, a następnie zmień Ustawienia sieciowe, aby maszyna wirtualna Kali znajdowała się w tej samej sieci, co inna maszyna wirtualna

Instalowanie i konfigurowanie Metasploitable2

Metasploitable2 został celowo skonstruowany tak, aby był podatny na ataki i ma na celu zapewnienie testerom penetracyjnym celu zawierającego luki w zabezpieczeniach, które mogą być wykorzystane do ćwiczenia testów penetracyjnych. Pobierasz Metasploitable2, dostarczony przez Rapid7, w następujących krokach.

UWAGA: Szczegółowe instrukcje instalacji można znaleźć na stronie www.hacking-tutorial.com/tips-and-trick/install-metasploitable-onvirtual-box/#sthash.2WTSpUII.dpbs. Jeśli adres URL nie działa, przejdź do strony www.hacking-tutorial.com i wyszukaj „install metasploitable on virtual box".

Metasploitable nie jest plikiem OVA. Rapid7 udostępnia wszystkie niezbędne pliki do utworzenia nowej maszyny wirtualnej w VirtualBox. Aby utworzyć maszynę wirtualną Metasploitable2 VirtualBox:

1. Użyj przeglądarki, aby przejść na stronę https://information.rapid7.com/download-metasploitable-2017.html. Musisz się zarejestrować, aby pobrać Metasploitable. Wypełnij formularz Pobierz teraz, a następnie kliknij przycisk PRZEŚLIJ. Po pomyślnej rejestracji zostaniesz przeniesiony na stronę pobierania. Kliknij przycisk POBIERZ METASPLOITABLE TERAZ, aby pobrać Metasploitable2. Jeśli pobieranie się nie rozpocznie, kliknij przycisk prawym przyciskiem myszy, skopiuj adres łącza, otwórz nową kartę w przeglądarce, a następnie wklej adres w pasku adresu. Pobieranie pliku powinno rozpocząć się automatycznie.

2. Użyj polecenia Wypakuj wszystko, aby wyodrębnić pliki instalacyjne ze skompresowanego pliku, który pobrałeś.

3. W VirtualBox kliknij Maszyna na pasku menu, a następnie kliknij Nowy. W oknie dialogowym Utwórz maszynę wirtualną wprowadź Nazwę, Typ, Wersję i Rozmiar pamięci maszyny wirtualnej.

4. Kliknij przycisk opcji Użyj istniejącego pliku dysku twardego wirtualnego, jeśli nie jest jeszcze wybrany.

5. Kliknij ikonę folderu w sekcji Dysk twardy, aby otworzyć okno Selektor dysku twardego.

6. Kliknij przycisk Dodaj i przejdź do wyodrębnionego folderu, aby znaleźć plik Metasploitable.vmdk. Musisz dodać ten plik do listy dysków twardych, aby użyć go z maszyną wirtualną Metasploitable2.

7. Wybierz plik Metasploitable.vmdk na liście dysków twardych, a następnie kliknij Wybierz.

8. Kliknij przycisk Utwórz, aby utworzyć maszynę wirtualną.

9. W VirtualBox kliknij prawym przyciskiem myszy maszynę wirtualną Metasploitable w prawym panelu, kliknij Uruchom w menu skrótów, a następnie kliknij Normalny start, aby uruchomić maszynę wirtualną Metasploitable. 10. Zaloguj się do Metasploitable VM, używając msfadmin jako nazwy użytkownika i msfadmin jako hasła

11. Wpisz ifconfig i naciśnij Enter. Zanotuj adres IP interfejsu eth0. Użyj tego adresu, aby wybrać maszynę wirtualną do testów penetracyjnych.

TWORZENIE RAPORTU Z TESTÓW PENETRACYJNYCH

Ostatecznym celem tego modułu jest zebranie informacji podczas działań związanych z testami penetracyjnymi, a następnie przedstawienie ustaleń w dokumencie raportu z testów penetracyjnych. Raport powinien zawierać następujące informacje:

• Szczegóły ustaleń

• Cele, które poddano testom penetracyjnym

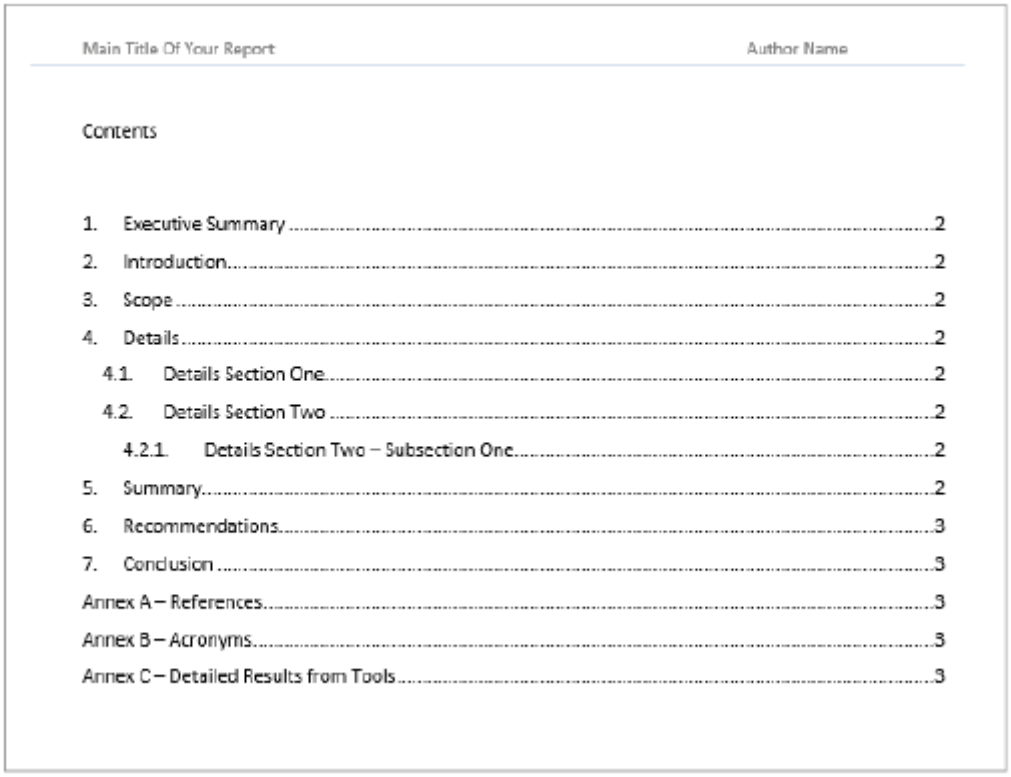
• Testy i narzędzia, których użyto

• Podsumowania, aby zapewnić czytelnikowi informacje przeglądowe

• Zalecenia i wnioski sugerujące, jak złagodzić wszelkie znalezione problemy z bezpieczeństwem W tym module używasz określonego formatu do tworzenia raportu z testów penetracyjnych, ale dostępne są inne formaty.

UWAGA : Przeszukaj Internet, aby znaleźć przykłady raportów z testów penetracyjnych i szablony, których możesz użyć. Na przykład zapoznaj się z następującą witryną, aby uzyskać przykładowy raport z testów penetracyjnych: www.offensive-security.com/reports/sample-penetration-testingreport. pdf. SANS Institute ma również dokument techniczny z wytycznymi dotyczącymi tworzenia raportu z testów penetracyjnych na stronie www.sans.org/white-papers/33343/.

W tym module używasz standardowego formatu raportu technicznego zawierającego informacje zorganizowane w sposób pokazany na rysunku.



Możesz utworzyć swój raport za pomocą programu Microsoft Word. Twój instruktor może mieć dostęp do szablonu dokumentu programu Word, który został już dla Ciebie utworzony.

W raporcie uwzględnij następujące sekcje i treści:

1. Streszczenie

Krótko podsumuj zakres testów oraz swoje ustalenia, zalecenia i wnioski w kilku krótkich akapitach. Grupą docelową są kadra kierownicza i menedżerowie, więc ogranicz żargon techniczny do minimum.

2. Wprowadzenie

Przedstaw temat raportu i jego cel. Omów cel testów penetracyjnych oraz sposób jego osiągnięcia i zademonstrowania. Ogólnie rzecz biorąc, tematem i celem raportu jest wyszukiwanie luk w jednym lub większej liczbie systemów komputerowych. Określ konkretne systemy, które testujesz. Celem jest znalezienie luk w systemach, a celem jest zaproponowanie możliwych rozwiązań dla tych luk.

3. Zakres

Jeśli kierujesz się tylko do określonego systemu lub zestawu systemów, opisz te informacje w sekcji zakresu. W przypadku testów penetracyjnych szczegóły zakresu obejmują cele, które testujesz, oraz rodzaje przeprowadzanych testów. Na przykład wskaż, czy wykonujesz pełne skanowanie Nessus pod kątem wszystkich luk, czy testujesz tylko jedną aplikację internetową.

4. Szczegóły

Sekcja szczegółów to najdłuższa część raportu, w której komunikujesz całą swoją pracę, odkrycia, kroki i wyniki. Przyjętą konwencją jest organizowanie i dzielenie szczegółów na wiele sekcji, podsekcji i nagłówków, w następujący sposób:

4.1. Sekcja szczegółów pierwsza

4.2. Sekcja szczegółów druga

4.2.1. Sekcja szczegółów druga – podsekcja pierwsza

W przypadku testów penetracyjnych zazwyczaj masz sekcję szczegółów dla każdego testowanego systemu (takiego jak każdy komputer). W podsekcjach opisz szczegóły określonych działań lub ustaleń (takich jak wyniki skanowania Nessus w tym systemie). Zawartość tych sekcji jest opisana bardziej szczegółowo w poniższych sekcjach. Jeśli pojedyncza aktywność ma wpływ na wiele systemów, na przykład skanowanie całej sieci za pomocą Nmap, możesz przechwycić wszystkie te szczegóły w jednej sekcji szczegółów, a następnie powtórzyć wyniki dla określonego celu w podsekcji dla tego celu. Każda sekcja szczegółów powinna podsumowywać wyniki z narzędzia, którego użyłeś do zebrania informacji. Pełna lista wszystkich wyników zebranych przez narzędzie nie jest pomocna i może być trudna do zrozumienia dla czytelnika. Wiele narzędzi dostarcza raporty podsumowujące i tabele ustaleń. Wyodrębnij te informacje i uwzględnij je w odpowiedniej sekcji szczegółów. Pełne listy wszystkich znalezionych informacji można później uwzględnić w dodatku lub dostarczyć jako plik pomocniczy na nośniku pamięci.

5. Podsumowanie

Podsumuj swoje ustalenia i stwórz ogólny komunikat na podstawie informacji zawartych w sekcji szczegółów. To nie jest twój wniosek; ta sekcja zawiera kilka akapitów podsumowujących. W przypadku raportu z testów penetracyjnych ta sekcja może składać się z oświadczeń podkreślających systemy, które pilnie potrzebują poprawek bezpieczeństwa i identyfikujących systemy uznane za dobrze zabezpieczone.

6. Zalecenia

Na podstawie pierwotnego celu, szczegółów, ustaleń i podsumowania stwórz uporządkowany zestaw zaleceń. Zalecenia te powinny obejmować kroki rozwiązywania problemów, upraszczania procedur i poprawy bezpieczeństwa. W raporcie z testów penetracyjnych zalecenia powinny określać kroki naprawy wszelkich luk w zabezpieczeniach znalezionych podczas testowania. Zwykle obejmują one stosowanie poprawek bezpieczeństwa, uaktualnianie systemów operacyjnych i oprogramowania, wzmacnianie serwerów poprzez usuwanie oprogramowania i stosowanie najlepszych praktyk.

7. Wnioski

Podsumuj cały dokument akapitem lub dwoma, które łączą ze sobą to, co ujawnił Twój cel, szczegóły, odkrycia i zalecenia.

Załącznik A – Odniesienia

Dołącz odniesienia do zewnętrznych źródeł informacji, o których wspomniałeś w swoim dokumencie, takich jak strony internetowe i książki.

Załącznik B – Akronimy

Jeśli raport używa wielu akronimów (zwłaszcza żargonu technicznego), pomocne może być dołączenie listy akronimów i definicji w osobnej sekcji.

Załącznik C – Szczegółowe wyniki z narzędzi

Jeśli używasz narzędzi, które gromadzą dużo danych jako podstawy swojego raportu (na przykład narzędzi do inwentaryzacji sieci lub narzędzi do oceny podatności), możesz dołączyć te dane w osobnej sekcji dla kompletności, być może w formacie tabeli. Podanie szczegółowych wyników pozwala czytelnikowi sprawdzić Twoje dowody. W testach penetracyjnych narzędzie Nessus może wygenerować raport ze wszystkich swoich ustaleń w formacie PDF lub HTML, a ten szczegółowy raport można wstawić tutaj.

Przed rozpoczęciem pracy laboratoryjnej nad testami penetracyjnymi utwórz ramy dokumentu raportu penetracyjnego, korzystając ze struktury opisanej w tej sekcji. W następnej sekcji przeprowadzasz testy penetracyjne i przechwytujesz informacje, które mają zostać uwzględnione w raporcie.

BAJTY BEZPIECZEŃSTWA

Nagrody za błędy to nagrody finansowe wypłacane przez organizacje osobom lub grupom, które odkrywają i zgłaszają wady w oprogramowaniu lub systemach komputerowych tej organizacji. Proces wykorzystywany do odkrywania wad to w zasadzie testy penetracyjne. W październiku 2021 r. Polygon, firma zajmująca się technologią blockchain, wypłaciła 2 miliony dolarów w nagrodach za błędy za lukę w zabezpieczeniach „podwójnego wydatku", która mogła spowodować spustoszenie w całej sieci. Luka została odkryta przez etycznego hakera o nazwisku Gerhard Wagner. Luka umożliwiła atakującemu podwojenie kwoty kryptowaluty, którą zamierzał wypłacić, nawet 233 razy. Ta wada mogła umożliwić złośliwemu aktorowi zdeponowanie tylko 4500 USD, a następnie natychmiastowe wypłacenie 1 miliona USD. Atakujący z 3,8 miliona USD mógłby wykorzystać lukę, aby zdobyć do 850 milionów USD. Najwyraźniej etyczne hakowanie się opłaca. Wygląda również na to, że przestępstwo się opłaca, ale etyczne hakowanie jest sprawiedliwe, a przestępstwo nie.

WYKONYWANIE TESTÓW PENETRACYJNYCH

Po uruchomieniu laboratorium testów penetracyjnych i przygotowaniu struktury raportów testów penetracyjnych możesz rozpocząć testowanie luk w zabezpieczeniach i rejestrowanie ustaleń. Następne sekcje przeprowadzą Cię przez szereg działań penetracyjnych.

Korzystanie z polecenia nmap

Jak się dowiedziałeś, nmap jest przydatnym narzędziem wiersza poleceń do wykrywania urządzeń komputerowych i ich otwartych portów w sieci. Możesz użyć informacji nmap do określania systemów docelowych za pomocą innych narzędzi skanujących, takich jak Nessus. Pamiętaj, że wykryte otwarte porty wskazują, które usługi są uruchomione w systemie docelowym, a co za tym idzie, jaki to może

być typ systemu. Na przykład, jeśli użyjesz nmap do przeskanowania systemu i odkryjesz, że porty 80 i 443 są otwarte, jest to dobry znak, że wykryłeś serwer WWW.

Przeprowadzanie skanowania Nmap w laboratorium testów penetracyjnych

Czas wymagany: 15 minut

Cel: Użyj Nmap, aby wykryć cele i otwarte porty w środowisku laboratorium testów penetracyjnych.

Opis: Pierwszym krokiem w testowaniu penetracyjnym środowiska laboratoryjnego jest uruchomienie skanowania nmap w celu wykrycia wszystkich celów i otwartych portów. Wyniki skanowania nmap zostaną uwzględnione i dodane do raportu.

1. Uruchom wszystkie maszyny wirtualne w środowisku laboratoryjnym. Upewnij się, że są podłączone do tej samej sieci.

2. Zaloguj się do maszyny wirtualnej Kali Linux.

3. Otwórz sesję terminala i użyj polecenia nmap, aby przeskanować wszystkie maszyny wirtualne w laboratorium testowym (w tym maszynę wirtualną Kali Linux). Wszystkie maszyny wirtualne laboratorium powinny znajdować się w tej samej podsieci sieciowej (być może 192.168.56.0), więc możesz użyć nmap do przeskanowania wszystkich maszyn wirtualnych jednocześnie, używając adresu sieciowego. Możesz również skanować każdą maszynę wirtualną indywidualnie, określając jej adres IP w poleceniu nmap. Logując się do każdej maszyny wirtualnej, możesz określić jej adres IP, czytając informacje na ekranie logowania lub używając polecenia ifconfig.

4. Przechwyć dane wyjściowe nmap i skopiuj je do raportu. Użyj narzędzia do przechwytywania ekranu, takiego jak Windows Snipping Tool lub Snip & Sketch, aby przechwycić obraz.

Korzystanie z polecenia netcat i metod HTTP

Przypomnijmy, że polecenie netcat (nc) i metody HTTP to przydatne narzędzia wiersza poleceń do wyodrębniania informacji z serwerów WWW. Informacje uzyskane z polecenia nc mogą ujawnić luki w zabezpieczeniach i mogą być używane do atakowania systemów za pomocą innych narzędzi skanujących, takich jak Nessus. Netcat ujawnia informacje, takie jak oprogramowanie serwera WWW, na którym uruchomiony jest cel, co może ujawnić luki w zabezpieczeniach.

Używanie polecenia netcat (nc) i metod HTTP do określania docelowych maszyn wirtualnych

Czas trwania: 15 minut

Cel: Użyj polecenia nc i metod HTTP, aby wyodrębnić informacje z serwerów WWW w środowisku laboratorium testów penetracyjnych.

Opis: Przynajmniej dwie maszyny wirtualne w środowisku laboratoryjnym to serwery WWW. Nessus jest zainstalowany na komputerze hosta wraz z serwerem WWW. Maszyna wirtualna Metasploitable jest podatnym na ataki serwerem WWW. Użyjesz polecenia netcat (nc) i metod HTTP, aby przeskanować każdą maszynę wirtualną i sprawdzić, jakie informacje o serwerze WWW możesz znaleźć. Wyniki dodasz do raportu.

1. Uruchom wszystkie maszyny wirtualne w środowisku laboratoryjnym. Upewnij się, że są podłączone do tej samej sieci wewnętrznej.

2. Zaloguj się do maszyny wirtualnej Kali Linux.

3. Uruchom sesję terminala.

4. Użyj polecenia nc i metod HTTP na każdej maszynie wirtualnej w środowisku laboratoryjnym (w tym na maszynie wirtualnej Kali Linux) i na komputerze hosta. Do wykonania tego zadania potrzebny będzie adres IP każdej maszyny wirtualnej i komputera hosta. Po połączeniu się z celem za pomocą polecenia nc użyj metod HTTP, takich jak GET i OPTIONS, aby zebrać informacje o każdej maszynie wirtualnej. Pamiętaj, aby wypróbować polecenie nc i metody HTTP na każdej maszynie wirtualnej i komputerze hostującym Nessus.

5. Przechwyć wyniki testów i skopiuj je do raportu. Użyj narzędzia do przechwytywania ekranu i przytnij obraz, aby pokazać wykonane polecenie i wyniki.

Korzystanie z polecenia wget

Przypomnijmy, że polecenie wget jest użytecznym narzędziem wiersza poleceń do wyodrębniania informacji z serwerów internetowych. Polecenie wget umożliwia pobieranie plików z serwera internetowego. Możesz zbadać te pliki, aby znaleźć luki w zabezpieczeniach, które można wykorzystać w innych narzędziach do testów penetracyjnych.

Używanie polecenia wget na maszynach wirtualnych w laboratorium testowym i komputerach docelowych

Czas wymagany: 15 minut

Cel: Użyj polecenia wget, aby spróbować pobrać pliki z maszyn wirtualnych docelowych w środowisku laboratorium testów penetracyjnych.

Opis: Możesz użyć polecenia wget, aby pobrać pliki z serwera WWW, takiego jak plik index.html, który często jest stroną główną witryny. Twoje działania nmap ujawniły, które porty są otwarte na każdej maszynie wirtualnej w laboratorium. Wszystkie maszyny wirtualne z otwartym portem 80 lub portem 443 to najprawdopodobniej serwery WWW, które powinieneś obrać za cel za pomocą polecenia wget. Dodaj zebrane wyniki do raportu.

1. Uruchom wszystkie maszyny wirtualne w środowisku laboratoryjnym. Upewnij się, że są podłączone do tej samej sieci.

2. Zaloguj się do maszyny wirtualnej Kali Linux.

3. Uruchom sesję terminala.

4. Uruchom wszystkie maszyny wirtualne w środowisku laboratoryjnym. Upewnij się, że są podłączone do tej samej sieci.

5. Użyj polecenia wget na każdej maszynie wirtualnej w środowisku laboratoryjnym i na komputerze hosta. Aby wykonać to zadanie, potrzebujesz adresu IP każdej maszyny wirtualnej i komputera hosta. Upewnij się, że używasz wget na każdej maszynie wirtualnej i na komputerze hostującym Nessus.

6. Przeanalizuj pliki przechwycone poleceniem wget i umieść wszelkie przydatne informacje z plików w swoim raporcie.

Korzystanie z polecenia enum4linux

Przypomnijmy, że polecenie enum4linux jest użytecznym narzędziem wiersza poleceń do enumeracji systemów Linux. Możesz użyć informacji uzyskanych z tego polecenia do określenia systemów docelowych za pomocą innych narzędzi do testów penetracyjnych, takich jak Nessus.

Używanie polecenia enum4linux do wyliczania celów

Czas wymagany: 15 minut

Cel: Użyj polecenia enum4linux do wyliczania celów w środowisku laboratorium testów penetracyjnych.

Opis: Polecenie enum4linux jest przydatne do zbierania informacji z maszyn opartych na systemie Linux. Twoja aktywność nmap mogła ujawnić system operacyjny Twoich celów, jeśli uwzględniłeś tę opcję w swoich skanach nmap. Zacznij od wybrania podejrzanych maszyn wirtualnych opartych na systemie Linux, a następnie użyj polecenia enum4linux na wszystkich maszynach wirtualnych i komputerze hosta. Dodaj wyniki ze skanów enum4linux do swojego raportu.

1. Uruchom wszystkie maszyny wirtualne w środowisku laboratoryjnym. Upewnij się, że są podłączone do tej samej sieci.

2. Zaloguj się do maszyny wirtualnej Kali Linux.

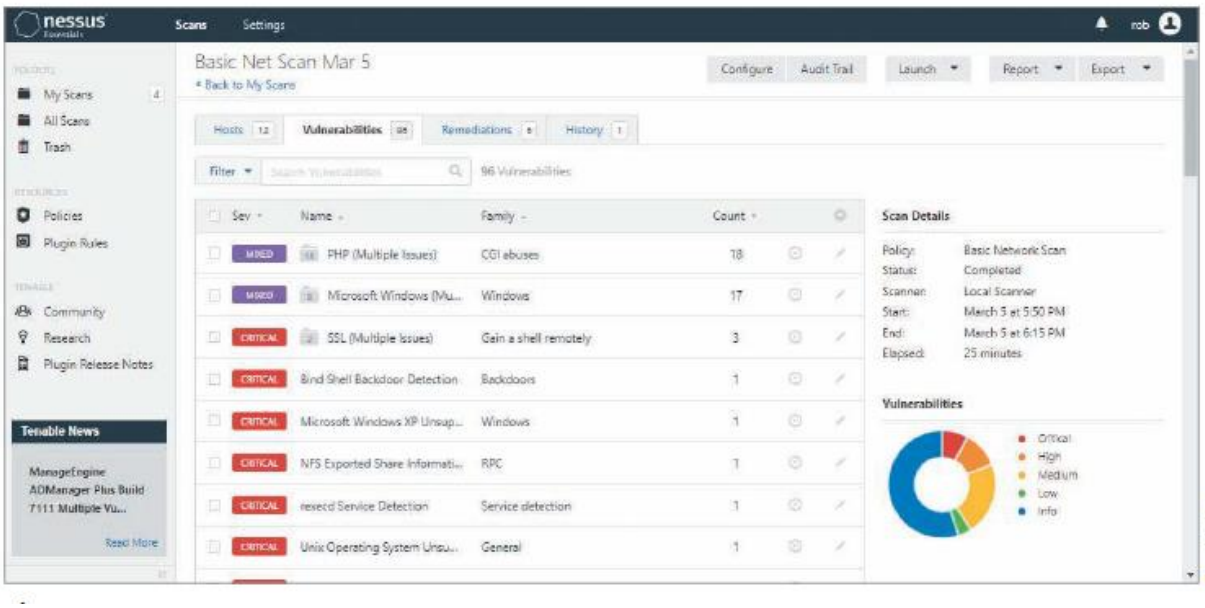
3. Uruchom sesję terminala.

4. Użyj polecenia enux4linux na każdej maszynie wirtualnej w środowisku laboratoryjnym i na komputerze hosta. Aby wykonać to zadanie, potrzebujesz adresu IP każdej maszyny wirtualnej i komputera hosta. Upewnij się, że używasz enum4linux na każdej maszynie wirtualnej i na komputerze hostującym Nessus.

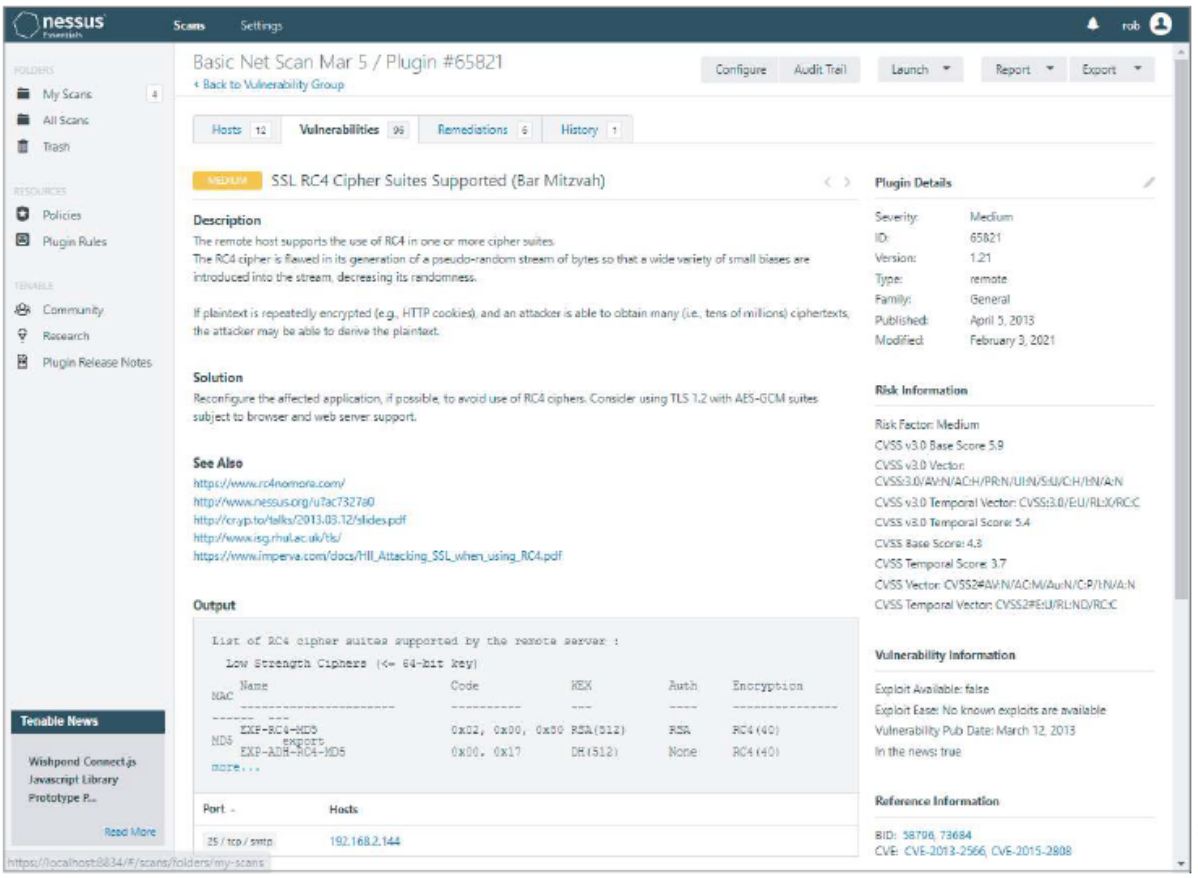
5. Przeanalizuj wyniki polecenia enum4linux i umieść wszelkie przydatne informacje w swoim raporcie.

Korzystanie z Nessus

Zainstalowałeś już Nessus Essentials na swoim komputerze, a w Ćwiczeniu 8-2 użyłeś go do przeskanowania lokalnego komputera z systemem Microsoft Windows. W tej sekcji użyjesz Nessus Essentials do przeskanowania wszystkich maszyn wirtualnych w środowisku laboratorium testów penetracyjnych. Możesz również przeskanować swój komputer osobisty, na którym zainstalowany jest Nessus. Pierwszym krokiem powinno być użycie Nessus do wykonania skanowania Host Discovery w sieci adapterów host-only i sprawdzenie, czy wykryje wszystkie maszyny wirtualne w środowisku laboratorium testów penetracyjnych. Wybierz sieć adapterów host-only (być może 192.168.56.0/24), a nie swoją rzeczywistą sieć. Następne kroki obejmują skanowanie każdej docelowej maszyny wirtualnej z osobna pod kątem luk w zabezpieczeniach. Wykonanie podstawowego skanowania sieci i ewentualnie skanowania testu aplikacji internetowych każdej maszyny wirtualnej ujawni wystarczające informacje do raportu. Aby odświeżyć pamięć, Rysunek pokazuje, gdzie można znaleźć wszystkie luki w zabezpieczeniach wykryte podczas skanowania.



Kliknij odkrytą lukę, a następnie przewiń w dół, aby odkryć numery CVE dla tej luki. Zobacz Rysunek



Informacje te będą przydatne później. Badanie luk w zabezpieczeniach na stronie internetowej CVE Strona internetowa cve.mitre.org jest przydatna do badania luk w zabezpieczeniach. Odwiedź stronę Search CVE List (https://cve.mitre. org/cve/search_cve_list.html), aby wyszukać luki w

zabezpieczeniach według określonego numeru CVE lub słów kluczowych. Użyj funkcji wyszukiwania w krajowej bazie danych luk NIST pod adresem https://nvd.nist.gov/vuln/search, aby przeprowadzić badanie luk w zabezpieczeniach. Informacje o raportach luk Nessus często zawierają linki do informacji o CVE znalezionych w krajowej bazie danych luk NIST. W Ćwiczeniu badasz niektóre CVE odkryte przez skanowanie Nessus. Wykonaj główne badanie na stronie cve.mitre.org i dołącz podsumowanie szczegółów do raportu. Możesz również uwzględnić informacje z NIST.

Kończenie raportu

Po przeprowadzeniu testów penetracyjnych nadszedł czas na sfinalizowanie raportu. Zbierz wszystkie zebrane informacje i dodaj kluczowe ustalenia do sekcji szczegółów raportu. Możesz uwzględnić wszystkie szczegóły w dodatku lub jako oddzielny plik danych. Przeanalizuj wyniki testów penetracyjnych i sformułuj podsumowanie, wnioski i zalecenia. Ponieważ raport zawiera wiele informacji i różne sekcje, utwórz spis treści, aby czytelnicy mogli szybko znaleźć to, czego szukają. Postępuj zgodnie ze wskazówkami podanymi w sekcji „Tworzenie raportu testów penetracyjnych" tego modułu, aby pomóc Ci ukończyć każdą sekcję raportu.

Skanowanie maszyn wirtualnych w laboratorium testów penetracyjnych za pomocą Nessus

Czas wymagany: 30 minut

Cel: skanowanie celów pod kątem luk w zabezpieczeniach za pomocą Nessus.

Opis: Nessus to potężne narzędzie do automatycznego wykrywania luk w zabezpieczeniach urządzeń komputerowych. Używasz Nessus do skanowania wszystkich maszyn wirtualnych w środowisku laboratorium testów penetracyjnych i dodawania wyników do raportu.

1. Uruchom wszystkie maszyny wirtualne w środowisku laboratorium. Upewnij się, że są podłączone do tej samej sieci wewnętrznej.

2. Zaloguj się do Nessus Essentials na komputerze hosta.

3. Wykonaj skanowanie Host Discovery w sieci adapterów host-only i sprawdź, czy wykryje wszystkie maszyny wirtualne w środowisku laboratorium testów penetracyjnych. Wybierz sieć adapterów host-only (być może 192.168.56.0/24), a nie swoją rzeczywistą sieć. Jak wyniki mają się do odcisku nmap z wiersza poleceń?

4. Utwórz i wykonaj skanowanie podstawowej sieci dla każdej maszyny wirtualnej w środowisku laboratorium testów penetracyjnych.

5. Utwórz i wykonaj skanowanie testu aplikacji internetowej dla każdej maszyny wirtualnej w środowisku laboratorium testów penetracyjnych.

6. Wyodrębnij informacje ze skanów, przechwytując ekrany lub używając narzędzia Wycinanie, aby skopiować obrazy tabel i wykresów wyświetlanych w Nessus. Dołącz wyniki skanowania do raportu. Możesz również użyć funkcji Raport w Nessus, aby utworzyć raport PDF lub HTML i dołączyć całość lub część raportu z testów penetracyjnych.

7. Przeskanuj komputer hosta pod kątem luk w zabezpieczeniach, ale dla własnego bezpieczeństwa nie dołączaj tych informacji do raportu.

Przeprowadzanie badań nad odkrytymi lukami

Czas wymagany: 30 minut

Cel: Użyj strony internetowej cve.mitre.org, aby zbadać szczegóły kilku luk CVE odkrytych przez skany Nessus.

Opis: Wiele luk odkrytych przez skany Nessus może zawierać odniesienia do CVE. Zbadaj kilka CVE uwzględnionych w wynikach. Nie musisz badać każdego CVE odkrytego przez Nessus, ale wybierz najpoważniejsze odkryte CVE i niektóre z najciekawszych.

1. Z wyników skanowania Nessus wybierz kilka numerów CVE do zbadania.

2. Otwórz przeglądarkę internetową i przejdź do https://cve.mitre.org/cve/search_cve_list.html.

3. W polu Wyszukaj listę CVE wprowadź dokładny numer CVE, a następnie kliknij Prześlij, aby rozpocząć wyszukiwanie.

4. Jeśli wyniki wyszukiwania zwrócą jakiekolwiek CVE, kliknij łącze CVE, aby wyświetlić szczegóły.

5. Dodaj do raportu część szczegółów, kopiując i wklejając wyniki lub używając Narzędzia wycinania do przechwytywania obrazów.

PRAKTYCZNE HACKOWANIE ETYCZNE PONOWNIE

Zajęcia w tym module wykorzystują tylko kilka narzędzi i metod omówionych wcześniej w tym kursie. Teraz, gdy masz środowisko laboratorium testów penetracyjnych, z którym możesz eksperymentować, możesz wypróbować niektóre z innych narzędzi i metodologii i zobaczyć, co ujawniają one na temat celów laboratorium. Możesz swobodnie przejrzeć każdy moduł ponownie i wypróbować narzędzia i metody opisane w tym module w środowisku laboratorium testów penetracyjnych. Dotarłeś do końca drogi w tym kursie, ale nadal masz daleką drogę do przebycia. Kontynuuj badanie tematu praktycznego hakowania etycznego i zbieraj więcej informacji na ten temat z różnych punktów widzenia. Przeszukaj Internet w poszukiwaniu przykładów i demonstracji różnych technik hakerskich omawianych w tym kursie. Podczas wyszukiwania technik hakerskich pamiętaj, aby postępować ostrożnie i unikać pobierania nieznanych narzędzi lub plików wykonywalnych. Demonstracje wideo i opisy tekstowe są stosunkowo bezpiecznymi źródłami samouczków hakerskich. Z wielką władzą wiąże się wielka odpowiedzialność, dlatego pamiętaj, aby zawsze mieć na sobie biały kapelusz, gdy będziesz korzystać ze swoich nowo nabytych umiejętności etycznego hakerstwa.

PODSUMOWANIE MODUŁU

• Oracle VirtualBox to idealny menedżer wirtualizacji do hostowania zbioru maszyn wirtualnych, które mają być używane jako cele testów penetracyjnych.

• OVA to skrót od Oracle Virtual Appliance. Urządzenie wirtualne to maszyna wirtualna, która została już zainstalowana na sprzęcie wirtualnym. Importowanie OVA jest wygodniejsze niż budowanie maszyny wirtualnej od podstaw.

• Metasploitable2 to maszyna wirtualna, która została celowo skonstruowana tak, aby była podatna na ataki. Metasploitable2 został stworzony przez Rapid7 i zapewnia testerom penetracyjnym cel zawierający luki w zabezpieczeniach, który można wykorzystać do ćwiczenia testów penetracyjnych.

• Raport z testów penetracyjnych powinien zawierać wstęp, szczegóły ustaleń, szczegóły testowanych celów, opisy użytych testów i narzędzi, podsumowania, aby zapewnić czytelnikowi skondensowane informacje, a także zalecenia i wnioski sugerujące, jak złagodzić wszelkie znalezione problemy z bezpieczeństwem.

• Pełna lista wszystkich wyników zebranych przez narzędzie nie jest pomocna i może być trudna do zrozumienia dla czytelnika, jeśli zostanie uwzględniona w sekcji szczegółów dokumentu testów penetracyjnych. Pełne listy wszystkich wyników mogą być zawarte w załączniku lub dostarczone jako plik pomocniczy na nośniku pamięci.

• Nagrody za błędy to nagrody finansowe wypłacane przez organizacje osobom lub grupom, które odkrywają i zgłaszają wady w oprogramowaniu lub systemach komputerowych danej organizacji.

• Witryna internetowa cve.mitre.org i funkcja wyszukiwania w krajowej bazie danych podatności NIST pod adresem https://nvd.nist.gov/vuln/search doskonale nadają się do badań nad podatnościami.