1. Atak D. Roberta osiągnął cel polegający na odmowie poprzez zamknięcie serwera WWW i uniemożliwienie dostępu do niego uprawnionym użytkownikom.

2. B. Pozwalając uczniom na zmianę własnych ocen, ta podatność stanowi drogę do nieautoryzowanej zmiany informacji. Brian powinien zalecić szkole wdrożenie mechanizmów kontroli integralności, które zapobiegają nieautoryzowanym modyfikacjom.

3. A. Robert udostępnił poufne informacje osobom i grupom, które nie były upoważnione do dostępu do tych informacji. To jest przykład ataku ujawniającego.

4. C. PCI DSS wymaga, aby organizacje przeprowadzały zarówno wewnętrzne, jak i zewnętrzne testy penetracyjne co najmniej raz w roku. Organizacje muszą również przeprowadzać testy po każdej znaczącej zmianie w środowisku danych posiadacza karty.

5. D. Wykorzystanie wewnętrznych zespołów testujących może wprowadzić świadome lub nieświadome uprzedzenia do procesu testów penetracyjnych. Ten brak niezależności jest jednym z powodów, dla których organizacje mogą zdecydować się na korzystanie z zewnętrznego zespołu testującego.

6. B. Okresowe powtarzanie testów penetracyjnych nie zapewnia organizacji korzyści kosztowych. W rzeczywistości wiąże się to z kosztami. Testy penetracyjne należy jednak powtarzać, ponieważ mogą wykryć problemy, które pojawiają się w wyniku zmian w testowanym środowisku i ewoluującym krajobrazie zagrożeń. Wykorzystanie nowych członków zespołu zwiększa również niezależność i wartość kolejnych testów.

7. A. W fazie planowania i określania zakresu testerzy penetracyjne i ich klienci powinni uzgodnić zasady zaangażowania w test. Powinno to skutkować pisemnym oświadczeniem o pracy, które jasno określa czynności dozwolone podczas testu penetracyjnego.

8. C. Zestawienie prac (SOW) obejmuje umowę roboczą między dwiema stronami i jest stosowane jako uzupełnienie istniejącej umowy lub umowy ramowej o świadczenie usług (MSA). NDA jest umową o zachowaniu poufności, a akronim MOD został wymyślony na to pytanie.

9. B. Język opisu usług sieci Web to oparty na języku XML język używany do opisu funkcjonalności zapewnianej przez usługę sieciową. XML jest powszechną podstawą dla wielu języków opisowych używanych do różnych definicji dokumentów i usług, z którymi może się zetknąć tester penetracyjny.

10. C. Testowanie białej skrzynki, znane również jako „kryształowe pudełko” lub „pełna wiedza”, zapewnia pełny dostęp i widoczność. Testowanie czarnoskrzynkowe nie dostarcza żadnych informacji, podczas gdy testowanie szarej skrzynki dostarcza ograniczonych informacji. Testowanie czerwonej skrzynki nie jest powszechnym terminem branżowym.

11. B. Umowa o zachowaniu poufności (NDA), obejmuje dane i inne informacje, które penetrator może napotkać lub odkryć podczas swojej pracy. Działa jako umowa prawna uniemożliwiająca ujawnienie tych informacji.

12. A. Zaawansowane trwałe zagrożenia (APT) to często organizacje sponsorowane przez państwo, posiadające znaczne zasoby i możliwości. Zapewniają najwyższy poziom zagrożenia na liście poziomów przeciwników.

13. D. Adres IP lub sieć, z której Robert wysyła swój ruch, najprawdopodobniej znalazła się na czarnej liście w ramach działań obronnych organizacji docelowej. Biała lista pozwoliłaby mu wejść i jest znacznie mniej prawdopodobne, że serwer lub sieć uległy awarii.

14. D. MOD został wymyślony na to pytanie, więc skanowanie Nmapa tego nie wygeneruje. Skanowanie Nmapa pokaże stan portów, zarówno TCP, jak i UDP.

15. D. Flaga axfr wskazuje na transfer strefy zarówno w narzędziach kopania, jak i hosta.

16. A. Robert wie, że porty TCP 139, 445 i 3389 są powszechnie używane dla usług Windows. Chociaż mogą być otwarte na urządzeniach z systemem Linux, Android lub iOS, Windows jest jego najlepszym wyborem.

17. A. Tylko skanowanie przez UDP spowoduje pominięcie jakichkolwiek usług TCP. Ponieważ zdecydowana większość obecnie używanych usług jest dostarczana jako usługi TCP, nie byłby to użyteczny sposób przeprowadzania skanowania. Ustawienie szybszego czasu skanowania (3 lub szybszego), zmiana ze skanowania połączenia TCP na skanowanie TCP SYN lub ograniczenie liczby testowanych portów to prawidłowe sposoby przyspieszenia skanowania. Robert musi być świadomy, co te zmiany mogą oznaczać, ponieważ szybkie skanowanie może zostać wykryte lub spowodować większe obciążenie sieci, a skanowanie mniejszej liczby portów może spowodować pominięcie niektórych portów.

18. D. Robert wie, że wielu administratorów systemu przenosi usługi ze swoich wspólnych portów usługowych do alternatywnych portów i że 8080 i 8443 są prawdopodobnie alternatywnymi portami serwerów HTTP (TCP 80) i HTTPS (TCP 443), i użyje przeglądarki internetowej do połącz się z tymi portami, aby je sprawdzić. Mógłby użyć Telnet do tych testów, ale wymaga to znacznie więcej pracy ręcznej, aby uzyskać ten sam wynik, co czyni go kiepskim drugim wyborem, chyba że nie ma innej opcji.

19. A. Exiftool jest przeznaczony do pobierania metadanych z obrazów i innych plików. Grep może być przydatny do wyszukiwania określonego tekstu w pliku, ale nie pobierze zakresu możliwych metadanych z pliku. PsTools to pakiet Windows Sysinternals, który zawiera różnorodne narzędzia zorientowane na procesy. Nginx to serwer WWW, system równoważenia obciążenia i wielozadaniowy stos usług aplikacji.

20. D. Identyfikacja systemu operacyjnego w Nmap opiera się na różnych atrybutach odpowiedzi. W tym przypadku Nmap najlepiej domyśla się, że na zdalnym hoście działa jądro Linuksa 2.6.9–2.6.33, ale nie może być bardziej szczegółowe. Nie określa dystrybucji, poziomu poprawek ani czasu ostatniej aktualizacji systemu.

21. C. Sqlmap to dedykowany skaner luk w zabezpieczeniach bazy danych i jest najbardziej odpowiednim narzędziem do użycia w tym scenariuszu. Ryan może odkryć te same luki w zabezpieczeniach za pomocą uniwersalnych skanerów Nessus lub OpenVAS, ale nie są to dedykowane narzędzia do skanowania luk w bazach danych. Nikto to skaner podatności aplikacji internetowych.

22. D. Pełne skanowanie prawdopodobnie dostarczy bardziej użytecznych i wykonalnych wyników, ponieważ obejmuje więcej testów. W scenariuszu nie ma wymogu, aby Robert unikał wykrycia, więc nie jest konieczne skanowanie z ukrycia. Jest to jednak test czarnej skrzynki, więc nie byłoby właściwe, aby Robert miał dostęp do skanów przeprowadzanych w sieci wewnętrznej.

23. A. Inwentaryzacja aktywów uzupełnia zautomatyzowane narzędzia o inne informacje służące do wykrywania systemów obecnych w sieci. Inwentaryzacja zasobów zawiera krytyczne informacje do skanowania podatności. Właściwe jest udostępnienie tych informacji testerom penetracyjnym podczas testu penetracyjnego białej skrzynki.

24. D. PCI DSS wymaga, aby organizacje przeprowadzały skanowanie podatności co najmniej raz na kwartał, chociaż wiele organizacji decyduje się na przeprowadzanie skanowania znacznie częściej.

25. B. QualysGuard, Nessus i OpenVAS to przykłady narzędzi do skanowania podatności. Snort to system wykrywania włamań.

26. A. Technologia szyfrowania prawdopodobnie nie będzie miała żadnego wpływu na wyniki skanowania luk w zabezpieczeniach, ponieważ nie zmienia usług udostępnianych przez system. Zapory sieciowe i systemy zapobiegania włamaniom mogą blokować przychodzący ruch skanowania, zanim dotrze on do systemów docelowych. Środowiska kontenerowe i zwirtualizowane mogą uniemożliwiać zewnętrznym skanerom wykrywanie usług w środowisku konteneryzowanym lub zwirtualizowanym.

27. B. Chociaż sieć może obsługiwać dowolny z tych protokołów, wewnętrzne luki w zabezpieczeniach ujawnienia IP występują, gdy sieć używa translacji adresów sieciowych (NAT) do mapowania publicznych i prywatnych adresów IP, ale serwer nieumyślnie ujawnia swój prywatny adres IP zdalnym systemom.

28. C. Metryka uwierzytelniania opisuje przeszkody uwierzytelniania, które osoba atakująca musiałaby usunąć, aby wykorzystać lukę w zabezpieczeniach.

29. C. Złożoność dostępu Niska wskazuje, że wykorzystanie podatność nie wymaga specjalnych warunków.

30. D. Jeśli którykolwiek z tych środków jest oznaczony jako C, dla Complete, oznacza to możliwość całkowitego włamania się do systemu.

31. D. Wersja 3.0 CVSS jest obecnie dostępna, ale nie jest tak szeroko stosowana jak bardziej powszechna wersja CVSS 2.0.

32. B. Ocena możliwości wykorzystania CVSS jest obliczana przy użyciu wektora dostępu, złożoności dostępu i metryk uwierzytelniania. Obliczenie nie uwzględnia wieku zagrożenia.

33. C. Podatności z wynikiem CVSSv2 wyższym niż 6,0, ale mniejszym niż 10,0 należą do kategorii wysokiego ryzyka.

34. B. TCP 445 jest portem usług zazwyczaj kojarzonym z usługami SMB.

35. A. Luka Ruby on Rails jest jedyną luką, która wyraźnie wspomina o zdalnym wykonaniu kodu, co najprawdopodobniej pozwoli Robertowi uzyskać dostęp do systemu.

36. B. Luka OpenSSH wyraźnie wskazuje, że umożliwia wyliczanie użytkowników, co czyni to najlepszym wyborem dla tego, co Robert chce osiągnąć.

37. C. Wyszukiwanie Metasploit obsługuje wiele popularnych systemów identyfikacji podatności, w tym CVE, BID i EDB, ale MSF został wymyślony na to pytanie. Może to brzmieć znajomo, ponieważ polecenie konsoli Metasploit to msfconsole.

38. A. Robert może bezpiecznie założyć, że prawie każdy nowoczesny system Linux będzie miał SSH, co czyni tunelowanie SSH uzasadnioną opcją. Jeśli łączy się z siecią wychodzącą z zaatakowanego systemu do swojego i tworzy tunel zezwalający na ruch, może użyć własnego skanera luk w zabezpieczeniach poprzez tunel, aby uzyskać dostęp do systemów zdalnych.

39. C. Robert użył narzędzia do zaplanowanych zadań, aby skonfigurować cotygodniowe uruchamianie av.exe z katalogu użytkownika o godzinie 9 rano Można założyć, że w tym przykładzie Robert uzyskał dostęp do katalogu użytkownika RKaramagi i umieścił swój własny av.exe i próbuje sprawić, by wyglądał nieszkodliwie, jeśli administratorzy go znajdą.

40. B. W większości systemów Linux plik /etc/passwd będzie zawierał listę użytkowników oraz ich katalogi domowe. Przechwytywanie zarówno /etc/passwd, jak i /etc/shadow jest ważne dla łamania haseł, czyniąc oba pożądane cele dla testerów penetracyjnych.

41. B. Kismet został specjalnie zaprojektowany do działania jako bezprzewodowy IDS oprócz innych funkcji bezprzewodowego przechwytywania pakietów. WiFite jest przeznaczony do audytu sieci bezprzewodowych, Aircrack zapewnia różnorodne narzędzia ataku oprócz możliwości przechwytywania i wstrzykiwania ruchu bezprzewodowego. SnortiFi zostało wymyślone na to pytanie.

42. C. Jeśli system NAC opiera się tylko na filtrowaniu adresów MAC, Robert musi tylko określić adres sprzętowy zaufanego systemu. Może to być dostępne po prostu patrząc na etykietę na laptopie lub komputerze stacjonarnym lub może być w stanie uzyskać ją za pomocą socjotechniki lub metod technicznych.

43. A. Aircrack-ng ma wbudowaną funkcjonalność fake-AP, z narzędziami, które pozwolą Robertowi zidentyfikować prawidłowe punkty dostępu, sklonować je, odłączyć system docelowy, a następnie działać jako pośrednik dla przyszłego ruchu.

44. A. Robert może używać spoofingu ARP do reprezentowania swojej stacji roboczej jako legalnego systemu, z którym inne urządzenia próbują się połączyć. Tak długo, jak jego odpowiedzi są szybsze, odbiera ruch i może działać jako człowiek pośrodku. Podsłuchiwanie sieci jest przydatne do odczytywania ruchu, ale samo w sobie nie jest przydatne w przypadku większości ruchu w sieci przełączanej. Powodzie SYN nie są przydatne do uzyskiwania danych uwierzytelniających, dlatego obie opcje C i D są nieprawidłowe.

45. D. Sfałszowanie przełącznika opiera się na interfejsie przełącznika, który jest skonfigurowany jako dynamiczny pożądany, dynamiczny auto lub tryb łącza trunkingowego, umożliwiając atakującemu generowanie komunikatów protokołu dynamicznego łącza trunkingowego. Atakujący może wtedy uzyskać dostęp do ruchu ze wszystkich sieci VLAN.

46. C. Bluejacking to technika ataku polegająca na próbie wysłania niechcianych wiadomości przez Bluetooth. Bluesnarfing próbuje wykraść informacje, podczas gdy Bluesniping to określenie dalekosiężnych ataków Bluetooth. Bluesending nie jest powszechnym terminem używanym dla ataków Bluetooth.

47. B. Ataki typu Pixie Dust wykorzystują brutalną siłę w celu zidentyfikowania klucza dla podatnych routerów z obsługą WPS ze względu na złe praktyki wyboru klucza. Inne opcje są wymyślone.

48. C. Wielorybnictwo to wyspecjalizowana forma phishingu, której celem są ważni przywódcy i personel wyższego szczebla. Gdyby Robert celował w konkretne osoby, byłby to spear phishing. Smishing używa wiadomości SMS, a VIPhishing został wymyślony na to pytanie.

49. B. Pułapka przepuszcza tylko jedną osobę na raz, z drzwiami na każdym końcu, które otwierają się i otwierają pojedynczo. Zapobiegnie to większości zachowań typu piggybacking lub tailgating, chyba że pracownicy będą świadomie niedbale.

50. D. Większość organizacji nadal wykorzystuje technologię RFID lub paski magnetyczne do kart dostępu, co ułatwia pracę testera penetracyjnego, ponieważ obie technologie można klonować. Karty inteligentne są znacznie trudniejsze do sklonowania, jeśli są prawidłowo zaimplementowane.

51. A. Robert podszywa się pod asystenta administracyjnego. Techniki przesłuchiwania są bardziej agresywne i stwarzają ryzyko, że cel stanie się obronny lub będzie świadomy, że jest przesłuchiwany.

Surfowanie przez ramię to proces patrzenia przez ramię w celu zdobycia informacji, a administracja nie jest terminem testowania penetracji.

52. B. Framework Exploitation Framework, czyli BeEF, to w szczególności przeznaczony do tego typu ataku. Robert może go użyć do łatwego wdrożenia narzędzi do wykorzystywania przeglądarki na złośliwej stronie internetowej, a następnie może użyć różnych technik phishingu i socjotechniki, aby skłonić pracowników RK do odwiedzenia tej witryny.

53. B. Robert powinien użyć narzędzia generatora nośników zakaźnych, które jest przeznaczone do tworzenia pendrive'ów i innych nośników, które można upuścić na miejscu, aby pracownicy mogli je odebrać. Moduł ataku Teensy USB HID może być kuszącą odpowiedzią, ale został zaprojektowany tak, aby Teensy (mały komputer podobny do Arduino) działał jak klawiatura lub inne urządzenie interfejsu ludzkiego, a nie tworzył zainfekowane nośniki. Tworzenie ataku na stronę internetową lub masowego ataku poczty nie jest częścią zrzutu klucza USB.

54. B. Podejścia do białej listy danych wejściowych definiują konkretny typ lub zakres danych wejściowych, które mogą dostarczyć użytkownicy. Kiedy programiści mogą napisać jasne reguły biznesowe definiujące dozwolone dane wejściowe użytkownika, biała lista jest zdecydowanie najskuteczniejszym sposobem zapobiegania atakom polegającym na wstrzykiwaniu.

55. D. Zapory sieciowe aplikacji internetowych muszą być umieszczone przed serwerami sieciowymi. Ten wymóg wyklucza lokalizację C jako opcję. Następną kwestią jest umieszczenie WAF tak, aby mógł filtrować cały ruch kierowany do serwera WWW, ale widział minimalną ilość obcego ruchu. To sprawia, że lokalizacja D jest najlepszą opcją do umieszczenia WAF.

56. A. Użycie polecenia SQL WAITFOR jest charakterystyczną cechą sygnatury ataku SQL wstrzykiwanego opartego na czasie.

57. A. Funkcja system() wykonuje ciąg poleceń w systemie operacyjnym z poziomu aplikacji i może być używana w atakach polegających na wstrzykiwaniu poleceń.

58. D. Testerzy penetracyjne mogą korzystać z wielu różnych źródeł w celu uzyskania dostępu do indywidualnych kont użytkowników. Mogą one obejmować przeprowadzanie ataków socjotechnicznych na indywidualnych użytkowników, uzyskiwanie zrzutów haseł z wcześniej przejętych witryn, uzyskiwanie domyślnych list kont i przeprowadzanie ataków łamania haseł.

59. B. Bilety przyznające bilety (TGT) są niezwykle cenne i można je tworzyć z wydłużonym okresem życia. Gdy atakującym uda się zdobyć TGT, TGT są często nazywane „złotymi biletami”, ponieważ umożliwiają pełny dostęp do systemów połączonych z protokołem Kerberos, w tym tworzenie nowych biletów, zmiany kont, a nawet fałszowanie kont lub usług.

60. B. Strony internetowe wykorzystują pliki cookie HTTP do utrzymywania sesji w czasie. Jeśli Robert jest w stanie uzyskać kopię pliku cookie sesji użytkownika, może użyć tego pliku cookie do podszywania się pod przeglądarkę użytkownika i przejęcia uwierzytelnionej sesji.

61. B. Customer Wordlist Generator, czyli CeWL, jest narzędziem zaprojektowanym do przeszukiwania witryny internetowej, a następnie tworzenia listy słów przy użyciu znalezionych plików i stron internetowych. Lista słów może być następnie użyta do pomocy w łamaniu haseł.

62. B. Najbardziej praktyczną odpowiedzią jest skompromitowanie interfejsu administracyjnego dla bazowego hipernadzorcy. Chociaż ucieczka VM byłaby przydatnym narzędziem, wykryto bardzo niewiele exploitów ucieczki VM, a każdy z nich został szybko załatany. Oznacza to, że testerzy penetracji

nie mogą polegać na tym, że jeden z nich jest dostępny i niezałatany, gdy napotkają hosta maszyny wirtualnej i powinni mieć docelowe prawa administracyjne i metody dostępu.

63. C. Litera s w -rwsr-xr-x wskazuje, że jest to plik binarny Set User ID (SUID), który umożliwia wykonanie pliku z uprawnieniami jego właściciela. Tutaj właścicielem i grupą jest root, więc ten plik prawdopodobnie nie będzie przydatny do eskalacji uprawnień i nie jest narzędziem, którego można użyć do zezwolenia na odwróconą powłokę.

64. A. Metasploit Meterpreter zawiera wbudowaną funkcjonalność Mimikatz, którą można wywołać za pomocą wywołania mimikatz_command -f. Użycie sampdump::hashes spowoduje zrzut bazy danych SAM, który można następnie złamać za pomocą różnych narzędzi.

65. D. Web Application Attack and Audit Framework (w3af) to narzędzie do testowania i wykorzystywania aplikacji internetowych, które może przechwycić witrynę i przetestować aplikacje oraz inne problemy z bezpieczeństwem, które mogą tam występować. Proxy Paros to doskonałe narzędzie internetowe proxy często używane przez testerów aplikacji internetowych, ale nie jest to pełnoprawny pakiet testowy, taki jak w3af. CUSpider i inne wersje Spidera to narzędzia służące do wyszukiwania wrażliwych danych w systemach, a Patator to narzędzie brutalnej siły.

66. C. Plik sudoers zazwyczaj znajduje się w katalogu /etc/sudoers w większości dystrybucji Linuksa.

67. C. W tym celu system Windows przeszuka katalog, w którym znajduje się aplikacja, bieżący katalog, katalog systemowy Windows, katalog Windows, a następnie katalogi wymienione w zmiennej PATH dla bibliotek DLL, jeśli nie ma na liście określonej lokalizacji pliku dla tego.

68. D. Interpretery PowerShell są dostępne na wszystkich głównych platformach, w tym Windows, Mac OS X i wielu popularnych wariantach Linuksa.

69. D. Polecenie print służy do generowania danych wyjściowych w Pythonie.

70. B. Polecenie Write-Host służy do generowania danych wyjściowych w PowerShell.

71. D. Ruby jest językiem programowania ogólnego przeznaczenia. Jest to język interpretowany, który wykorzystuje skrypty, a nie język skompilowany, który wykorzystuje kod źródłowy do generowania plików wykonywalnych.

72. D. Musisz ustawić bit użytkownika (właściciela) na wykonanie (x), aby umożliwić wykonanie skryptu Bash. Zadanie to wykonuje polecenie chmod u+x.

73. C. Zasady RemoteSigned umożliwiają wykonanie dowolnego skryptu PowerShell, który piszesz na komputerze lokalnym, ale wymaga, aby skrypty pobrane z Internetu były podpisane przez zaufanego wydawcę.

74. A. PowerShell wymaga użycia $ przed nazwą tablicy w operacji przypisania. Elementy tablicy są następnie dostarczane jako lista oddzielona przecinkami. Opcja B działałaby w Bash, podczas gdy opcja C działałaby w Ruby lub Pythonie.

75. D. Poświadczenie ustaleń jest poświadczeniem wydanym przez testerów penetracyjnych w celu udokumentowania, że przeprowadzili test i jego wyniki dla celów zgodności.

76. A. Rozwiązanie Local Administrator Password Solution (LAPS) firmy Microsoft zapewnia metodę randomizacji poświadczeń konta administratora lokalnego poprzez integrację z usługą Active Directory.

77. C. Trzy najczęstsze wyzwalacze komunikacji podczas testu penetracyjnego to zakończenie etapu testowania, odkrycie krytycznego wyniku oraz identyfikacja wskaźników wcześniejszego naruszenia. Dokumentacja nowego testu nie jest normalnym wyzwalaczem komunikacji.

78. B. Jedynym wnioskiem, jaki Robert może wyciągnąć z tych informacji jest to, że serwer oferuje niepotrzebne otwarte usługi, ponieważ nasłuchuje połączeń SSH, podczas gdy nie powinien obsługiwać tej usługi.

79. B, C. Podczas pentestu jest wielu interesariuszy, którzy mogą być zainteresowani wynikami i sukcesem zaangażowania. Zazwyczaj grupa ta składa się z kierownictwa wykonawczego, działu kontraktowego lub prawnego, pracowników ochrony, działu IT i pentesterów.

80. A, C. Analiza wpływu jest formalnym podejściem do oceny wymagania, plusy i minusy podjęcia określonego kierunku działania oraz budżet organizacyjny i ograniczenia techniczne to dwa obszary zainteresowania, które wpływają na decyzję o kontynuowaniu zadania typu pentest.