1. A. Cain i Abel, Hashcat i John the Ripper to narzędzia do łamania haseł. OWASP ZAP to internetowe narzędzie proxy.

2. D. Nikto jest narzędziem do oceny bezpieczeństwa aplikacji internetowych o otwartym kodzie źródłowym. Sqlmap testuje aplikacje internetowe, ale testuje tylko pod kątem podatności na wstrzyknięcie SQL. OpenVAS i Nessus to uniwersalne skanery luk w zabezpieczeniach. Chociaż mogą wykrywać problemy z bezpieczeństwem aplikacji internetowych, nie są specjalnie zaprojektowane do tego celu.

3. OLLYDBG, WinDBG i IDA to narzędzia do debugowania obsługujące środowiska Windows. GDB to narzędzie do debugowania specyficzne dla Linuksa.

4. C. Na etapie działań na cele atakujący wykonuje czynności, które były celem ataku. Jako taki jest to ostatni etap w łańcuchu.

5. B. Polowanie na zagrożenia zakłada, że organizacja została już naruszona i wyszukuje oznaki udanych ataków.

6. B. Podczas ostatniego etapu testu penetracyjnego, raportowania i komunikowania wyników, testerzy dostarczają strategie łagodzenia problemów zidentyfikowanych podczas testu.

7. B. Oceny są ważne tylko wtedy, gdy się pojawiają. Systemy ulegają ciągłym zmianom z powodu poprawek, zmian użytkowników i zmian konfiguracyjnych. Oświadczenie Roberta o ważności punktu w czasie jest kluczowym elementem w umowach zlecenia na testy penetracyjne.

8. A. Testowanie czarnoskrzynkowe jest często nazywane testowaniem „wiedzy zerowej”, ponieważ testerzy nie mają żadnej wiedzy na temat systemów lub ich ustawień, jak w przypadku testów białoskrzynkowych lub nawet ograniczonej wiedzy zapewnianej przez test szarej skrzynki.

9. B. Przypinanie certyfikatu wiąże hosta z certyfikatem X.509 lub kluczem publicznym. Reszta odpowiedzi została zmyślona!

10. C. Chociaż ISO lub sponsor mogą być właściwym organem podpisującym, ważne jest, aby Robert zweryfikował, czy osoba, która podpisuje, faktycznie jest właściwym organem podpisującym w organizacji. Oznacza to, że ta osoba musi mieć uprawnienia do poddania organizacji testowi penetracyjnemu. Niestety nie jest to termin prawny, więc Robert być może będzie musiał odrobić pracę domową ze swoim sponsorem projektu, aby upewnić się, że wszystko przebiegnie prawidłowo.

11. B, C. Zarówno kompleksowość testu, jak i ograniczenie, że ma on znaczenie tylko w momencie jego przeprowadzenia, są właściwymi zastrzeżeniami, które Robert może uwzględnić. Tolerancja ryzyka i wpływu ocenianej organizacji powinna być wykorzystana do określenia zakresu i zasad zaangażowania w ocenę.

12. C. Robert ma ograniczone informacje o swoim celu, co oznacza, że prawdopodobnie przeprowadza ocenę szarej skrzynki. Gdyby miał pełną wiedzę, przeprowadzałby ocenę białą lub kryształową skrzynią. Gdyby nie miał wiedzy, byłaby to ocena z czarnej skrzynki.

13. A. Ocena czerwonego zespołu aktywnie stara się zachowywać jak atakujący, a strategia czarnej skrzynki oznacza, że atakujący nie ma wcześniejszej wiedzy ani informacji o organizacji. To najlepiej symuluje wysiłki rzeczywistego napastnika, aby przeniknąć do zabezpieczeń organizacji.

14. C. Centrum Informacji Sieci Afrykańskiej (AFRINIC) jest Regionalnym Rejestrem Internetowym (RIR) dla Afryki. Réseaux IP Europé (RIPE) obejmuje Azję Środkową, Europę, Bliski Wschód i Rosję. Amerykański rejestr numerów internetowych (ARIN) obejmuje Stany Zjednoczone, Kanadę, części

regionu Karaibów i Antarktydę. Centrum informacyjne sieci Azji i Pacyfiku (APNIC) obejmuje Azję, Australię, Nową Zelandię i inne kraje regionu. Centrum informacyjne sieci Ameryki Łacińskiej i Karaibów (LACNIC) obejmuje regiony Ameryki Łacińskiej i Karaibów.

15. B. Większość nowoczesnych wdrożeń SNMP używa innych niż domyślny ciąg wspólnoty. Jeśli Robert nie będzie miał prawidłowego ciągu społeczności, nie otrzyma informacji, których szuka. Jeśli port 25 wyglądał na atrakcyjną odpowiedź, prawdopodobnie myślisz o SMTP. Posiadanie zestawu prywatnego ciągu SNMP nie zatrzyma zapytania Roberta, jeśli ma on właściwy ciąg wspólnoty, ale nie posiadanie odpowiedniego ciągu wspólnoty to zrobi.

16. B. Robert wydał polecenie, które prosi hping o przesłanie ruchu SYN (-S) w trybie szczegółowym (-V) do remotesite.com na porcie 80.

17. C. Seria trzech gwiazdek podczas traceroute oznacza, że zapytanie hosta nie powiodło się, ale ruch przechodzi. Wiele hostów jest skonfigurowanych tak, aby nie odpowiadać na tego typu ruch, ale prawidłowo kierować ruchem.

18. A. Okulary BGP są publicznie dostępnymi usługami, które umożliwiają inspekcję trasy. Robert powinien znaleźć serwis z lustrami BGP i zapytać o trasy dla swojego celu.

19. B. Testerzy penetracji zawsze szukają wskaźników niewłaściwej konserwacji. Leniwi lub nieuważni administratorzy częściej popełniają błędy, które umożliwiają testerom penetracji.

20. D. Wszystkie te narzędzia z wyjątkiem ExifTool są użyteczne jako skanery portów z pewnym sprytnym zastosowaniem:

Hping: hping example.com -V --scan 1-1024

NETCAT: nc -zv example.com 1-2014

Telnet: Telnet do każdego portu w poszukiwaniu pustego ekranu

21. B. Robert przeprowadza statyczną analizę kodu poprzez przeglądanie kodu źródłowego. Dynamiczna analiza kodu wymaga uruchomienia programu, a zarówno testowanie mutacji, jak i fuzzing to rodzaje analizy dynamicznej.

22. C. Robert powinien najpierw przeprowadzić skanowanie w środowisku testowym, aby zidentyfikować prawdopodobne luki w zabezpieczeniach i ocenić, czy sam skan może zakłócić działalność biznesową.

23. C. Chociaż raportowanie i komunikacja są ważnymi elementami zarządzania podatnościami, nie są one uwzględniane w cyklu życia. Trzy fazy cyklu życia to wykrywanie, naprawa i testowanie.

24. A. Ciągłe monitorowanie obejmuje dane z podejść opartych na agentach do wykrywania luk w zabezpieczeniach i raportuje zmiany konfiguracji związane z bezpieczeństwem na platformie zarządzania lukami, gdy tylko się pojawią, zapewniając możliwość analizy tych zmian pod kątem potencjalnych luk w zabezpieczeniach.

25. B. Systemy mają umiarkowany wpływ z punktu widzenia poufności, jeżeli można oczekiwać, że nieuprawnione ujawnienie informacji będzie miało poważny negatywny wpływ na działalność organizacyjną, aktywa organizacyjne lub osoby.

26. A. Common Vulnerability Scoring System (CVSS) zapewnia znormalizowane podejście do pomiaru i opisywania dotkliwości luk w zabezpieczeniach. Robert mógłby użyć tego systemu punktacji do priorytetyzacji problemów zgłaszanych przez różne systemy źródłowe.

27. B. Testerzy penetracyjni powinni zawsze zapoznać się z opisem pracy (SOW) w celu uzyskania wskazówek, jak postępować w sytuacjach, w których odkryją krytyczne podatności. Zakres prac może wymagać natychmiastowego zgłoszenia tych problemów kierownictwu lub może umożliwić kontynuację testu wykorzystującego lukę.

28. D. TLS 1.1 to bezpieczny protokół transportowy obsługujący ruch sieciowy. Wszystkie pozostałe wymienione protokoły mają wady, które sprawiają, że są niepewne i nie nadają się do użytku.

29. B. Certyfikaty cyfrowe mają na celu dostarczenie publicznych kluczy szyfrujących i nie spowoduje to błędu. Wszystkie pozostałe okoliczności są powodem do niepokoju i mogą wywołać alert podczas skanowania luk w zabezpieczeniach.

30. D. W zwirtualizowanym centrum danych na sprzęcie hosta wirtualnego działa specjalny system operacyjny zwany hiperwizorem, który pośredniczy w dostępie do podstawowych zasobów sprzętowych.

31. A. Luki w zabezpieczeniach maszyn wirtualnych to najpoważniejszy problem, jaki może wystąpić w środowisku zwirtualizowanym, szczególnie gdy na wirtualnym hoście działają systemy o różnych poziomach bezpieczeństwa. W ataku polegającym na ucieczce osoba atakująca ma dostęp do jednego hosta wirtualnego, a następnie udaje mu się wykorzystać ten dostęp, aby włamać się do zasobów przypisanych do innej maszyny wirtualnej.

32. B. Systemy wykrywania włamań (IDS) to kontrola bezpieczeństwa używana do wykrywania ataków na sieć lub hosta. Internet rzeczy (IoT), systemy nadzoru i akwizycji danych (SCADA) oraz systemy sterowania przemysłowego (ICS) są powiązane z podłączaniem obiektów świata fizycznego do sieci.

33. D. W ataku typu cross-site scripting (XSS) osoba atakująca osadza w witrynie internetowej polecenia skryptów, które zostaną później wykonane przez niczego niepodejrzewającego użytkownika odwiedzającego witrynę. Chodzi o to, aby nakłonić użytkownika odwiedzającego zaufaną witrynę do wykonania złośliwego kodu umieszczonego tam przez niezaufaną stronę trzecią.

34. A. W ataku typu SQL injection napastnik stara się wykorzystać aplikację internetową w celu uzyskania dostępu do podstawowej bazy danych. Charakterystyczne dla tych ataków są średniki i apostrofy.

35. B. Robert włączył zdalny dostęp PowerShell, znany jako PSRemoting i skonfigurował go tak, aby zezwalał na nieszyfrowane sesje przy użyciu podstawowego uwierzytelniania. Ta konfiguracja powinna zaniepokoić każdego administratora Windows, który ją znajdzie!

36. A. Choć może się to wydawać dziwne, wykorzystanie informacji do zbierania exploitów na wczesnym etapie może pomóc w uzyskaniu przydatnych informacji dla innych exploitów. Ponadto większość exploitów zbierających informacje pozostawia bardzo niewiele dowodów i może dostarczać informacji na temat konfiguracji usług i kont użytkowników, co czyni je bardzo przydatnym narzędziem w sytuacji takiej jak opisany scenariusz.

37. C. Spośród wymienionych opcji, najlepszym rozwiązaniem Roberta jest prawdopodobnie upadek z pendrive'a. Dostarczanie pendrive'ów ze złośliwym oprogramowaniem do różnych lokalizacji wokół celu może spowodować podłączenie jednego lub więcej, a staranne projektowanie może zachęcić personel w docelowej organizacji do klikania wybranych przez niego pakietów złośliwego oprogramowania. Gdy lokalna stacja robocza zostanie skompromitowana za pomocą narzędzia, które może się z nim skontaktować, będzie miał środki poza istniejącymi zabezpieczeniami, co prawdopodobnie pozwoli mu znaleźć inne luki w sieci organizacji.

38. C. Tryb przechwytywania SMB Metasploit, Responder i Wireshark mogą przechwytywać skróty SMB z transmisji. Imppacket nie zawiera tej możliwości, ale zapewnia szeroką gamę powiązanych narzędzi, w tym możliwość uwierzytelniania za pomocą skrótów po ich przechwyceniu. Jeśli zastanawiasz się, czy na egzaminie napotkasz tego typu pytania, pamiętaj o wyeliminowaniu odpowiedzi, których jesteś pewien, aby zmniejszyć liczbę pozostałych opcji. Tutaj można się domyślić, że Metasploit ma do tego moduł, a Wireshark jest narzędziem do przechwytywania pakietów, więc przechwytywanie ruchu rozgłoszeniowego może wymagać pracy, ale jest możliwe. To sprowadza cię do szansy 50/50.

39. A. Robert musi użyć exploita z oceną Excellent, czyli najwyższym poziomem, na którym exploity Metasploit mogą być sklasyfikowane. Exploity, które są niższe niż ten poziom, mogą powodować ryzyko awarii usługi.

40. B. Tęczowe tabele to listy wstępnie obliczonych skrótów dla wszystkich możliwych haseł dla danego zestawu reguł haseł. Narzędzia tabel tęczowych porównują skróty z wcześniej obliczonymi skrótami, które odpowiadają znanym wartościom haseł. Odbywa się to za pomocą stosunkowo szybkiego wyszukiwania w bazie danych, umożliwiającego szybkie „złamanie" zaszyfrowanych haseł, nawet jeśli haszy nie są odwracalne.

41. D. Robert używa zagnieżdżonych znaczników wewnątrz pakietu do próby przeskoku sieci VLAN. Jeśli mu się powiedzie, jego pakiety zostaną dostarczone do systemu docelowego, ale nie zobaczy żadnej odpowiedzi.

42. C. Wysłanie FIN i ACK podczas podszywania się pod docelową stację roboczą spowoduje zamknięcie połączenia. Spowoduje to, że cel będzie próbował nawiązać mniej bezpieczne połączenie, jeśli jest obsługiwane.

43. A, D. Aby w pełni zachowywać się jak człowiek pośrodku, Robert musi sfałszować zarówno serwer, jak i cel, aby każdy z nich myślał, że jego komputer to system, do którego wysyłają. Sfałszowanie bramy (10.0.1.1) lub adresu rozgłoszeniowego (255.255.255.255) nie będzie służyć jego celom.

44. B. Polecenia net systemu Windows mogą wyświetlać wiele informacji o domenie lokalnej, a politykę haseł można przejrzeć za pomocą polecenia net accounts /domain.

45. Odpowiedź wstrzyknięcia B. Roberta była zbyt wolna, ponieważ musi dotrzeć przed legalny serwer DNS. Jeśli jego czas nie jest odpowiedni, uzasadniona odpowiedź zostanie zaakceptowana.

46. A. Karty RFID o niskiej częstotliwości są często używane jako karty dostępu i można je łatwo klonować za pomocą niedrogich urządzeń do klonowania towarów. Karty średniej częstotliwości w zakresie od 400 do 451 kHz nie istnieją, podczas gdy karty o wysokiej częstotliwości są bardziej skłonne do klonowania przy użyciu funkcji NFC telefonu. Karty o ultrawysokiej częstotliwości są mniej znormalizowane, przez co klonowanie jest bardziej złożone.

47. A. Niedobór może być silnym motywatorem podczas próby socjotechniki. Wiadomość e-mail, którą wysłał Robert, wykorzysta ograniczoną liczbę nagród pieniężnych do motywowania respondentów. Gdyby dodał „pierwsze pięć", skupiłby się również na pilności, która często łączy się z niedoborem, aby zapewnić dodatkową motywację.

48. C. Próba quid pro quo polega na tym, że inżynier społeczny oferuje coś o postrzeganej wartości, tak aby odbiorca czuł się wobec niego dłużnikiem. Następnie obiekt docelowy jest proszony o wykonanie działania lub wykonanie w inny sposób tego, czego oczekuje od niego tester penetracyjny.

49. D. Robert użył ataku wodopoju, ale popełnił także krytyczny błąd. Umieszczanie złośliwego oprogramowania w witrynie innej firmy, do której ma dostęp wiele osób w okolicy (lub poza nią),

prawdopodobnie wykracza poza zakres jego zaangażowania i jest prawdopodobnie nielegalne. Lepszym planem byłoby skupienie się na zasobach posiadanych i obsługiwanych przez samą firmę, do których dostęp mają wyłącznie pracownicy wewnętrzni.

50. C. Kiedy penetrator zostanie złapany, jego pierwszą odpowiedzią powinno być podanie pretekstu. Udana próba socjotechniki w tym momencie może uratować próbę penetracji. Jeśli to nie zadziała, wezwanie kontaktu organizacyjnego w celu uzyskania odpowiedzi „wyjdź z więzienia na wolność" może być jedyną opcją w trudnej sytuacji.

51. A. Klucze USB są czasami nazywane fizycznymi pułapkami miodu. Kuszą pracowników do podłączania nieznanych urządzeń do swoich komputerów, czego dobrze wyszkolony i podejrzliwy personel nie powinien robić. Pozostałe opcje zostały wymyślone dla tego pytania.

52. B. Robert posługuje się pojęciem wzajemności, aby przekonać pracownika, że powinien wykonać działanie, które przyniesie mu korzyść, ponieważ wyświadczył mu przysługę.

53. C. Surfowanie przez ramię przybiera wiele form, w tym obserwowanie, jak pracownik wpisuje kod dostępu. Setec Astronomy to nawiązanie do doskonałego filmu o hakowaniu Sneakers, podczas gdy zarówno nadzór kodu, jak i przechwytywanie klawiatury zostały wymyślone na to pytanie.

54. C. Problem czasu od sprawdzenia do czasu użycia (TOCTTOU lub TOC/TOU) to sytuacja wyścigu, która występuje, gdy program sprawdza uprawnienia dostępu zbyt daleko przed żądaniem zasobu.

55. A. Podpisywanie kodu zapewnia programistom sposób na potwierdzenie

autentyczność ich kodu dla użytkowników końcowych. Programiści używają funkcji kryptograficznej do cyfrowego podpisywania kodu własnym kluczem prywatnym, a następnie przeglądarki mogą używać klucza publicznego programisty do weryfikacji tego podpisu i upewnienia się, że kod jest zgodny z prawem i nie został zmodyfikowany przez nieupoważnione osoby.

56. A. YASCA (Yet Another Source Code Analyzer) to kod źródłowy analizatora służący do wykonywania statycznej analizy aplikacji. Brzoskwinia to narzędzie do fuzzingu, które jest rodzajem analizy dynamicznej. Immunity i WinDBG to debugery, kolejna klasa narzędzi do dynamicznego testowania bezpieczeństwa.

57. B. ZAP (Zed Attack Proxy) to proxy przechwytujące opracowane przez Open Web Application Security Project (OWASP). Użytkownicy ZAP mogą przechwytywać żądania wysyłane z dowolnej przeglądarki internetowej i zmieniać je przed przekazaniem ich do serwera WWW.

58. A. Korzystanie z API może zostać ograniczone poprzez przypisanie uprawnionym użytkownikom unikalnych kluczy API, które zapewniają im dostęp, z zastrzeżeniem ich własnych ograniczeń autoryzacji i ograniczeń przepustowości.

59. B. GDB to szeroko stosowany debugger typu open source dla platformy Linux. WinDBG i OllyDbg są również debuggerami, ale są dostępne tylko dla systemów Windows. SonarQube to narzędzie do ciągłej oceny bezpieczeństwa i nie jest debugerem.

60. C. Ten adres URL zawiera adres lokalnego pliku przekazanego do sieci aplikacji jako argument. Najprawdopodobniej jest to exploit wykorzystujący lokalne pliki, który próbuje uruchomić złośliwy plik, który testerzy wcześniej przesłali na serwer.

61. C. Robert potrzebuje fizycznego dostępu do systemu. Niektóre ataki z zimnym rozruchem wykorzystują bardzo niskie temperatury, aby zapewnić dłuższy okres czasu, w którym dane można odzyskać z modułów pamięci, ale dostęp fizyczny jest absolutnie wymagany.

62. C. Pliki instalacji nienadzorowanej obejmują administratora lokalnego hasła przechowywane w postaci zwykłego tekstu lub Base-64. Robert może łatwo uzyskać hasła z tych plików za pomocą narzędzia enum_unattend Metasploit lub ręcznie, jeśli zechce.

63. D. Deweloperzy często nieumyślnie pomijają cudzysłowy lub zapominają o prawidłowym wymijaniu cudzysłowów, umożliwiając testerom penetracyjnym wstawienie programów w ścieżce, które będą wykonywane zamiast żądanej usługi. Robert powinien umieścić w ścieżce swój własny program, a następnie spróbować spowodować ponowne uruchomienie usługi lub systemu, zastępując działającą legalną usługę własnym.

64. D. Patator, Hydra i Medusa to przydatne narzędzia do brutalnej siły. Minotaur może być świetną nazwą dla narzędzia do testowania penetracji, ale autorzy tej książki nie znają żadnego narzędzia o nazwie Minotaur, które jest używane przez testerów penetracji!

65. C. Robert ustawił powłokę wiążącą, która łączy powłokę z portem usługi. Odwrotna powłoka zainicjowałaby połączenie z zaatakowanego hosta do jego stacji roboczej do testowania penetracji (lub innego systemu, do którego Robert ma dostęp). Pytanie nie dostarcza wystarczających informacji, aby określić, czy powłoka może być powłoką korzeniową, a ślepa powłoka nie jest powszechnym terminem w testach penetracyjnych.

66. B. Jeśli Robert ma odpowiednie tablice tęczy dla metody haszowania i zestawu znaków hasła, Rainbow Crack powinien być najszybszy. Hashcat byłby drugim najszybszym, jeśli korzysta z potężnej karty graficznej, a John the Ripper będzie zwykle najwolniejszą z wymienionych metod łamania haseł. CeWL jest generatorem list słów lub słowników i nie jest narzędziem do łamania haseł.

67. B. Kod zawiera nawiasy klamrowe, więc oczywiście jest napisany w PowerShell.

68 .D. Kod zawiera stwierdzenie fi, jest oczywiście napisane w Bash.

69. C. Kod zawiera dwukropki, jest to oczywiście kod Pythona.

70. D. Polecenie nc pozwala otworzyć port sieciowy do nasłuchiwania, a następnie skierować dane wejściowe otrzymane na tym porcie do pliku lub pliku wykonywalnego.

71. D. PowerShell, Python i Ruby obsługują warianty klauzuli try..catch. Bash nie zapewnia wbudowanej możliwości obsługi błędów.

72. C. Wartość %26 służy do kodowania znaków ampersand w adresie URL przy użyciu schematu kodowania procentowego.

73. B. Operator -ge sprawdza, czy jedna wartość jest większa lub równa innej wartości w Bash i PowerShell, podczas gdy operator -gt sprawdza, czy jedna wartość jest ściśle większa od drugiej. Operatory >= i > są używane w Ruby i Pythonie do tych samych celów.

74. C. Trzy główne kategorie działań naprawczych to ludzie, proces i technologia. Testowanie nie jest częścią naprawy.

75. A. Sanityzacja danych wejściowych (znana również jako walidacja danych wejściowych) i zapytania parametryczne są akceptowalnymi środkami zapobiegania atakom typu SQL injection. Zapory sieciowe generalnie nie zapobiegłyby takiemu atakowi.

76. B. Utwardzanie systemu powinno mieć miejsce podczas początkowej budowy systemu i okresowo w trakcie jego eksploatacji. Nie ma potrzeby wzmacniania systemu przed wycofaniem z eksploatacji, ponieważ jest on w tym momencie zamykany.

77. B. Techniki uwierzytelniania biometrycznego wykorzystują pomiar pewnych cech fizycznych użytkownika, takich jak skanowanie odcisków palców, rozpoznawanie twarzy lub analiza głosu. To jest „coś, czym jesteś”.

78. C. Identyfikatory zestawu usług (SSID) to nazwy nadawane w celu jednoznacznej identyfikacji sieci bezprzewodowej i nie mogą wprowadzać ani białej, ani czarnej listy.

79. A. Zakres prac określa czynności pracy związane z projektem.

80. B. Dokument dotyczący zasad zaangażowania (RoE) można znaleźć w Zakresie Prac lub może być całkowicie osobnym artefaktem. Ten dokument przedstawia przepisy dotyczące zaangażowania i sposobu, w jaki może przebiegać wykonanie pentestu. Po otrzymaniu pisemnego upoważnienia w RoE, zespół pentest może przystąpić do egzaminu.