1. D. Zasady zaangażowania (ROE) powinny być jasno określone i podpisane przez obie strony przed rozpoczęciem testu penetracyjnego. Brak ROE naraża Twoją organizację na potencjalne spory sądowe, jeśli coś pójdzie nie tak podczas procesu testowania. Weryfikacja nowego klienta następuje podczas procesu określania zakresu testu i tworzenia dokumentu ROE. MSA określa warunki, które będą regulować przyszłe umowy.

2. D. Przed przeprowadzeniem testu penetracyjnego musisz uzyskać pisemną zgodę od kierownictwa wyższego szczebla organizacji docelowej na przeprowadzenie testu. Uzyskiwanie zgody ustnie lub e-mailem jest generalnie niedopuszczalne. Uzyskiwanie pozwolenia od personelu IT jest również generalnie nie do przyjęcia.

3. A. W teście penetracyjnym wykorzystującym czarną skrzynkę tester nie ma wcześniejszej wiedzy na temat celu. Dlatego najlepiej symuluje to, co wydarzyłoby się podczas ataku z zewnątrz. Testy penetracyjne białej i szarej skrzynki pozwalają testerowi uzyskać pewien stopień wcześniejszej wiedzy na temat celu.

4. A. W teście penetracyjnym szarej skrzynki tester posiada częściową wiedzę na temat celu. Można to wykorzystać do symulacji złośliwego ataku wewnętrznego przeprowadzanego przez przeciętnego pracownika. W teście penetracyjnym w czarnej skrzynce tester nie ma wcześniejszej wiedzy na temat celu. W teście białoskrzynkowym tester ma rozległą wiedzę na temat celu.

5. C. Ponieważ tester penetracyjny nie ma wiedzy na temat celu, przeprowadzenie testu czarnej skrzynki zajmuje najwięcej czasu i pieniędzy. W przeciwieństwie do tego, testy szarej i białej skrzynki są zwykle tańsze i zajmują mniej czasu, ponieważ tester ma pewien poziom wiedzy na temat celu.

6. A. Znaki *** na wyjściu polecenia traceroute wskazują, że router dla tego konkretnego przeskoku trasy działa i przekazuje ruch, ale nie może odpowiadać na pingi używane przez polecenie traceroute.

7. C i D. Z tą nazwą domeny jest powiązany serwer sieciowy. To jest skonfigurowane do korzystania z protokołu HTTP (niezabezpieczony) na porcie 80 i protokołu HTTPS (zabezpieczony).

8. D i E. W tym przykładzie certyfikat SSL/TLS organizacji został podpisany przy użyciu funkcji skrótu kryptograficznego SHA256. Ponadto widać, że organizacja korzysta z serwera internetowego IIS, który działa na bazie Windows Server.

9. A. W tym przykładzie wiersz o treści „250 2.1.5 Recipient OK” wskazuje, że jest to prawidłowy adres e-mail w domenie organizacji docelowej. Nie ujawnia jednak, do kogo należy adres. Wiesz tylko, że to prawdziwy e-mail. Aby użyć go w teście penetracyjnym, musisz najpierw dokonać triangulacji z listą dyrektorów firmy, taką jak czasami znajduje się na stronie internetowej organizacji.

10. B. W tym przykładzie wiersz o treści „250 2.1.5 Recipient OK” wskazuje, że jest to prawidłowy adres e-mail w domenie organizacji docelowej. Ponieważ jest to prawidłowy adres e-mail, teraz wiesz, że organizacja najprawdopodobniej używa konwencji nazewnictwa e-maili pierwsze_początkowe+nazwisko@nazwa_firmy.com. Korzystając z tych informacji, możesz odwołać się do strony internetowej z biogramami wykonawczymi organizacji i stworzyć adresy e-mail dla wszystkich członków zespołu zarządzającego.

11. C. Ludzie mogą być zmotywowani do szybkiego działania, gdy wierzą, że coś, czego chcą, jest w ograniczonej ilości. Nazywa się to niedoborem. Nie chcą przegapić okazji, produktu, transakcji lub usługi, która wkrótce stanie się niedostępna.

12. A. Ludzie mogą być zmotywowani do działania, jeśli myślą, że wszyscy robią to samo. Nazywa się to dowodem społecznym. (Błędnym) założeniem jest to, że jeśli wszyscy inni coś robią, to musi to być właściwe.

13. C. Ludzie są w naturalny sposób motywowani szacunkiem dla władzy. Kiedy wierzą, że ktoś z władzy chce, aby coś zrobili, często zastosują się do tego, zwłaszcza jeśli prośba jest połączona z poczuciem pilności.

14. B. Wiele osób ma naturalną motywację do pomagania innym w niebezpieczeństwie. Nazywa się to pilnością. Kiedy uważają, że ktoś potrzebuje pomocy, mogą nagiąć lub złamać zasady, aby pomóc tej osobie.

15. A. Większość ludzi pomoże komuś, kogo postrzegają jako przyjaciela. Nazywa się to podobieństwem. Kiedy ktoś, kogo uważają za przyjaciela, potrzebuje pomocy, mogą nagiąć lub złamać zasady, aby pomóc tej osobie.

16. C. Opcja –T2 powoduje, że nmap skanuje w trybie kontroli. Ten typ skanowania działa dość wolno. Jednak powolność sprawia również, że skanowanie jest trudniejsze do wykrycia.

17. B. Opcja –oN powoduje, że nmap zapisuje wynik skanowania do standardowego pliku tekstowego. Za pomocą tej opcji musisz określić nazwę pliku.

18. A. Opcja –oX powoduje, że nmap zapisuje dane wyjściowe ze skanowania do pliku tekstowego w formacie XML. Za pomocą tej opcji musisz określić nazwę pliku.

19. D. Opcja –oG powoduje, że nmap zapisuje wynik skanowania do pliku tekstowego w formacie umożliwiającym jego szybkie przeszukiwanie za pomocą polecenia grep. Za pomocą tej opcji musisz określić nazwę pliku.

20. C. Opcja –oA powoduje, że nmap zapisuje wynik skanowania do normalnego pliku tekstowego, w pliku tekstowym w formacie XML oraz do pliku tekstowego z możliwością grppowania. Za pomocą tej opcji należy określić podstawową nazwę pliku. Do każdego z plików wygenerowanych przy użyciu tej podstawowej nazwy pliku zostanie dodane inne rozszerzenie. Normalny plik będzie miał rozszerzenie .nmap, plik grppable będzie miał rozszerzenie .gnmap, a plik XML będzie miał rozszerzenie .xml.

21. C. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś wymienić wykryte luki w sekcji raportu „Wyniki i środki zaradcze” wraz ze sposobem ich znalezienia.

22. C. Tworząc swój pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś wymienić wykryte luki w sekcji raportu „Wyniki i środki zaradcze” wraz z informacją o tym, jak je znalazłeś i co klient może zrobić, aby naprawić problem . W tym przykładzie zaleca się zainstalowanie aktualizacji MS17-010-Critical firmy Microsoft w tej sekcji.

23. D. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś zgłosić swoje oceny ryzyka w sekcji Metryki i miary. Oceny te pozwalają czytelnikowi ustalić priorytety zagrożeń, a także dokonać porównań między testami penetracyjnymi przeprowadzanymi w czasie.

24. E. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś zgłosić swoje zalecenia w sekcji Wnioski.

25. C. Informacje zawarte w części „Wyniki i środki zaradcze” w pisemnym raporcie z ustaleń będą zwykle ograniczone apetytem klienta na ryzyko. Na przykład organizacja z apetytem na większe ryzyko może chcieć, abyś zawierał tylko informacje o wykrytych lukach wysokiego lub krytycznego ryzyka i nie zgłaszał luk o średnim lub niskim ryzyku.

26. B. To jest przykład przeniesienia ryzyka. Zamiast uniknąć ryzyka, przenosząc się do nowej lokalizacji lub złagodzić ryzyko za pomocą sejsmicznych modernizacji obiektu, klient przeniósł ryzyko na firmę ubezpieczeniową.

27. D. W tym scenariuszu klient ustalił, że ryzyko jest akceptowalne i nie podejmie środków w celu jego kontrolowania. Zwykle dzieje się tak, gdy organizacja ustali, że koszt usunięcia lub kontrolowania ryzyka przewyższa koszt incydentu bezpieczeństwa wynikającego z tego ryzyka.

28. B. Ponieważ jest to test penetracyjny zgodności, najpierw musisz uzyskać dostęp do standardów PCI-DSS i przejrzeć wymagania, aby klient został uznany za „zgodnego". Zazwyczaj organizacja zarządzająca publikuje listy kontrolne, których należy użyć do oceny zgodności. Te listy kontrolne będą miały duży wpływ na zakres, budżet i harmonogram testu.

29. A i B. Payment Card Industry Data Security Standard (PCI-DSS) to zestaw zabezpieczeń, które firmy muszą wdrożyć w celu ochrony danych kart kredytowych. Na przykład dwa wymagania określają, że organizacja musi ograniczyć fizyczny dostęp do wszystkich danych posiadacza karty oraz że sieć CDE musi być odizolowana od reszty sieci.

30. B i E. Standard bezpieczeństwa danych dotyczących kart płatniczych (PCI-DSS) to zestaw zabezpieczeń, które firmy muszą wdrożyć w celu ochrony danych kart kredytowych. Na przykład dwa wymagania określają, że wszystkie dane posiadacza karty muszą być zaszyfrowane przed przesłaniem na nośnik sieciowy oraz że wszystkie hasła domyślne zostaną usunięte z wdrożonego sprzętu i oprogramowania.

31. A. Skanowanie wykrywające ma na celu proste mapowanie każdego systemu w sieci docelowej. Jako taki używa bardzo nieinwazyjnych mechanizmów (takich jak ping) do wyliczania sieci.

32. B. Pełne skanowanie sprawdza każdy host wykryty w sieci docelowej. Ponieważ wykorzystuje do tego natrętne metody, pełne skanowanie jest zwykle szybko wykrywane (i prawdopodobnie blokowane) przez urządzenia IDS lub IPS.

33. A. Skanowanie wykrywające ma na celu proste mapowanie każdego systemu w sieci docelowej przy użyciu bardzo nieinwazyjnych mechanizmów (takich jak ping) w celu wyliczenia sieci. Z tego powodu ten typ skanowania jest najmniej prawdopodobny do wykrycia przez urządzenie IDS lub IPS.

34. B. Pełne skanowanie przesłuchuje każdego hosta wykrytego w sieci docelowej przy użyciu inwazyjnych metod. Pełne skanowanie jest zwykle szybko wykrywane (i prawdopodobnie blokowane) przez urządzenia IDS lub IPS. Z tego powodu obrońca chętniej użyje pełnych skanów do dokładnego przetestowania swojej sieci. Tester penetracyjny rzadziej korzysta z pełnego skanowania, ponieważ może zostać wykryty tak szybko. Wyjątkiem byłby test białej skrzynki, w którym wszyscy spodziewają się, że tester penetracyjny będzie przeprowadzał skanowanie podatności.

35. C. Skanowanie stealth zlicza hosty w sieci docelowej, wysyłając im pakiet SYN. Jeśli zostanie odebrany pakiet SYN-ACK, skaner wie, że host docelowy istnieje. SYNACK zawiera również ograniczoną ilość informacji o hoście, które mogą zostać przechwycone i przeanalizowane przez skaner.

36. A. W ataku SSL stripping użytkownik wysyła żądanie HTTPS do serwera WWW. Ma to na celu zapewnienie, że komunikacja między serwerem a przeglądarką jest szyfrowana. Jednak exploit oszukuje serwer sieciowy, myśląc, że użytkownik chce standardowego połączenia HTTP i nawiązywana jest niezaszyfrowana sesja. Jeśli użytkownik nie obserwuje uważnie, może nie zdawać sobie sprawy, że tak się stało.

37. C. Najlepszym sposobem obrony przed atakiem SSL stripping jest zaimplementowanie zasady HTTP Strict Transport Security (HSTS), które uniemożliwiają przeglądarce użytkownika otwieranie strony internetowej, chyba że do przesłania strony z serwera WWW do klienta użyto połączenia HTTPS.

38. B. W tym przykładzie miał miejsce atak typu man-in-the-middle w dół, ponieważ SSL 2.0 jest mniej bezpieczny niż TLS 1.2. Jeśli użytkownik nie jest wyjątkowo czujny, prawdopodobnie nie zauważy, że do ochrony sesji zamiast TLS używany jest protokół SSL.

39. A. Wysyłając fałszywe wiadomości ARP, stacja robocza testera może oszukać klienckie stacje robocze, myśląc, że jest serwerem sieciowym, łącząc adres IP serwera z adresem MAC stacji roboczej. Podobnie serwer może zostać oszukany, myśląc, że jego stacja robocza jest stacją roboczą użytkownika końcowego, robiąc to samo, wysyłając fałszywą wiadomość ARP do serwera mapującego adres IP klienta na adres MAC jej stacji roboczej.

40. A. Zalewając serwer półotwartymi połączeniami TCP, które nigdy się nie kończą, tester sprawia, że nie ma on wystarczających zasobów do obsługi uzasadnionych żądań sieciowych. Ponieważ do przeprowadzenia testu warunków skrajnych użyto tylko jednego hosta, jest to przykład standardowego ataku typu odmowa usługi (DoS).

41. D. Narzędzie ncat jest zaktualizowaną i ulepszoną wersją starszego narzędzia netcat.

42. A lub B. Do skonfigurowania exploita powłoki wiązania można użyć narzędzia zdalnego dostępu ncat lub netcat.

43. C. Narzędzie Drozer zapewnia pełną strukturę audytu bezpieczeństwa i ataków, zaprojektowaną wyłącznie dla urządzeń mobilnych z systemem operacyjnym Android.

44. B. APK Studio to narzędzie, którego można użyć do inżynierii wstecznej pliku wykonywalnego APK i przeanalizowania go pod kątem luk w zabezpieczeniach.

45. A. Android APK Decompilation for the Lazy (APKX) to wrapper Pythona, który może wyodrębnić kod źródłowy Java bezpośrednio z pliku wykonywalnego APK Androida.

46. D. Uwierzytelnianie dwuskładnikowe (2FA) wymaga od użytkowników dostarczania czynników z dwóch różnych kategorii. W takim przypadku wymaganie od użytkownika podania nazwy użytkownika (coś, co wiesz), kodu PIN (coś, co wiesz) i skanu rozpoznawania twarzy (coś, czym jesteś) stanowi uwierzytelnianie 2FA.

47. B. Uwierzytelnianie trójskładnikowe (3FA) wymaga od użytkowników dostarczania czynników z trzech różnych kategorii. W takim przypadku wymaganie od użytkownika podania nazwy użytkownika (coś, co wiesz), kodu PIN (coś, co wiesz), skanu odcisku palca (coś, czym jesteś) i jednorazowego hasła (coś, co masz) stanowi uwierzytelnianie 3FA.

48. A. W tym scenariuszu możesz zalecić, aby aplikacja była przepisana tak, że wszystkie dane wejściowe użytkownika są oczyszczane przed przesłaniem do bazy danych zaplecza. Załóżmy na przykład, że aplikacja zawiera pole, w którym użytkownicy powinni wprowadzić swój numer telefonu. Programiści mogli sprawdzić, czy wprowadzone informacje zawierają tylko liczby (i tylko prawidłową liczbę dla numeru telefonu). Zapobiega to złośliwym napastnikom od przesyłania instrukcji SQL do tych pól, które mogą potencjalnie ujawnić informacje w bazie danych.

49. A. W tym scenariuszu możesz zalecić, aby aplikacja była przepisana tak, że dane są escapowane. Ucieczka to proces zabezpieczania danych poprzez usuwanie niechcianych informacji, takich jak zniekształcony kod HTML lub znaczniki skryptu. Zapobiega to postrzeganiu danych jako kodu. Ucieczka

danych pomaga zabezpieczyć informacje przed udostępnieniem ich użytkownikowi końcowemu i zapobiega wstrzykiwaniu kodu SQL oraz atakom typu cross-site scripting.

50. C. Używanie sparametryzowanych zapytań jest zwykle uważane za lepszą ochronę przed atakami typu SQL injection niż oczyszczanie danych wejściowych użytkownika. W przypadku zapytań parametrycznych przygotowane instrukcje są używane ze zmiennymi ograniczonymi w celu uzyskania dostępu do bazy danych SQL.

51. C. W tym scenariuszu klient poprosił Cię o wyjście poza uzgodniony zakres testów. Jest to przykład pełzania zakresu, który jest częstym zjawiskiem w kontraktowaniu IT. W tym scenariuszu możesz odpowiedzieć na dwa sposoby. Po pierwsze, możesz po prostu odrzucić żądanie jako wykraczające poza zakres. Alternatywnie możesz poprosić klienta o włączenie serwerów poczty e-mail do aneksu do istniejącej umowy za dodatkową opłatą.

52. A. Standard PCI-DSS jest standardem branżowym zapewniającym, że organizacje przetwarzające karty kredytowe spełniają określone wymagania bezpieczeństwa. Ponieważ testujesz zgodność klienta z tymi wymaganiami, przeprowadzasz ocenę opartą na zgodności.

53. C. Umowa testowa powinna zawierać zastrzeżenie wskazujące, że test jest ważny tylko w momencie jego przeprowadzenia, ponieważ przyszłe zmiany technologiczne mogą ujawnić nowe luki, które są obecnie nieznane. Nie możesz ponosić odpowiedzialności, jeśli nowe exploity lub luki w zabezpieczeniach pojawią się później po zakończeniu testu.

54. B. Ilość informacji wykrytych w teście penetracyjnym w dużym stopniu zależy od zasad zaangażowania i rodzaju zastosowanej oceny. Na przykład test białej skrzynki zwykle dostarcza bardziej kompletnych informacji niż test czarnej skrzynki. Podobnie, jeśli określone systemy i urządzenia zostaną zidentyfikowane jako poza zakresem, wszelkie luki, które zawierają, nie zostaną wykryte. Ten język umowy ma na celu ochronę użytkownika w przypadku wykrycia luki w systemie poza zakresem po zakończeniu testu.

55. A. Test czarnej skrzynki jest czasami określany jako ocena zerowej wiedzy, ponieważ testerzy penetracji mają niewielką lub żadną wiedzę o sieci klienta. Ten rodzaj oceny najlepiej naśladuje rzeczywisty atak zewnętrzny.

56. A i B. Pierwszą odpowiedzią na brak najlepszych praktyk klienta byłoby wykorzystanie urządzeń z domyślnymi nazwami użytkownika i hasłami w późniejszym teście penetracyjnym. Następnie powinieneś zalecić klientowi przyjęcie lepszych najlepszych praktyk w raporcie końcowym.

57. A i D. Zamiast kupować system Windows, możesz po prostu utworzyć kod exploita w swoim systemie Linux, a następnie skompilować go krzyżowo tak, aby mógł działać na systemach Windows. Dostępne są różne narzędzia Linux, które mogą to zrobić za Ciebie.

58. B i D. W tym scenariuszu najpierw zmapowałeś luki znalezione w skanach na możliwe exploity. Następnie zmodyfikowałeś te exploity, aby działały na starszych systemach operacyjnych dla serwerów.

59. C. W tym scenariuszu połączyłeś ze sobą kilka exploitów, aby złamać system docelowy. Nazywa się to łańcuchem exploitów.

60. B. W tym scenariuszu musisz przetestować zmodyfikowany exploit przed faktycznym atakiem na serwery docelowe, aby upewnić się, że działa i nie ma żadnych niezamierzonych konsekwencji. Skutecznym sposobem, aby to zrobić, jest wykorzystanie informacji z wyliczenia do odtworzenia

systemów docelowych jako maszyn wirtualnych w środowisku laboratoryjnym i przetestowania zmodyfikowanego exploita. Proces ten nazywa się opracowywaniem dowodu koncepcji.

61. A. Usługa podsystemu lokalnych organów bezpieczeństwa (LSASS) to proces działający w systemie Windows w celu wymuszenia zasad bezpieczeństwa w systemie. Weryfikuje użytkowników logujących się do systemu, zarządza zmianami haseł użytkowników, tworzy tokeny dostępu i wprowadza wpisy do dziennika zabezpieczeń.

62. A. Uruchamianie nienadzorowanych instalacji przez sieć przy użyciu środowiska Preboot Execution Environment (PXE) może potencjalnie skutkować przesyłaniem poświadczeń uwierzytelniających w postaci zwykłego tekstu. Podczas instalacji nienadzorowanej do automatyzacji procesu instalacji używany jest specjalny plik zwany plikiem odpowiedzi. Jeśli plik odpowiedzi zawiera informacje o koncie użytkownika, które mają zostać utworzone w systemie podczas instalacji, informacje te są przesyłane w postaci zwykłego tekstu.

63. D. Baza danych SAM w systemie Windows zawiera zaszyfrowane hasła do kont lokalnych. Domyślnie znajduje się w C:\Windows\System32\config\. Jeśli można wykonać kopię tego pliku, można go złamać za pomocą wielu różnych narzędzi dostępnych w Internecie w celu ujawnienia zawartych w nim haseł.

64. D. To jest przykład exploita przejmującego kontrolę nad biblioteką DLL. Złośliwa biblioteka DLL prawdopodobnie zawiera te same funkcje, co oryginalna biblioteka DLL, umożliwiając aplikacjom, które na niej polegają, poprawne działanie. Jednak może również zawierać złośliwy kod, który jest wykonywany podczas ładowania biblioteki DLL.

65. A i B. Używanie niecytowanych ścieżek do usług jest jednym ze sposobów wykorzystania usług w systemie Windows. Bez cytowania ścieżek do usług wszelkie spacje w nazwie katalogu nie będą przetwarzane poprawnie i mogą spowodować załadowanie złośliwego pliku wykonywalnego usługi umieszczonego celowo w wynikowej niecytowanej ścieżce katalogu zamiast prawidłowego pliku wykonywalnego usługi. Ponadto zapisywalne pliki wykonywalne usług można zastąpić złośliwymi plikami wykonywalnymi o tej samej nazwie pliku.

66. C. Dodanie TargetHost = gets line do skryptu Rubiego powoduje, że akceptuje on dane wprowadzone w wierszu poleceń przez użytkownika i przypisuje je do zmiennej o nazwie TargetHost.

67. D. Dodanie linii puts TargetHost do skryptu Rubiego powoduje wyświetlenie na ekranie wartości zmiennej o nazwie TargetHost.

68. A. Dodanie wiersza TargetHost = input('Proszę wprowadzić nazwę hosta:') do skryptu Pythona powoduje, że akceptuje on dane wejściowe wprowadzone w wierszu poleceń przez użytkownika i przypisuje je do zmiennej o nazwie TargetHost.

69. B. Dodanie linii print (TargetHost) do skryptu Rubiego powoduje wyświetlenie na ekranie wartości zmiennej o nazwie TargetHost.

70. B. Element #!/bin/bash musi być zawarty na początku każdego skryptu powłoki Bash.

71. A. Najlepszą rekomendacją byłoby wyłączenie wszelkich niepotrzebnych usług. Niepotrzebne usługi mogą stanowić zagrożenie dla bezpieczeństwa, ponieważ zwiększają powierzchnię ataku sieciowego klienta, zapewniając potencjalnemu napastnikowi wiele sposobów na wykorzystanie systemu. Powierzchnia ataku to łączna suma luk w danym urządzeniu komputerowym lub sieci, które są dostępne dla potencjalnego hakera.

72. A. Rozwiązanie hasła administratora lokalnego (LAPS) to narzędzie firmy Microsoft, które zarządza poświadczeniami administracyjnymi. Służy do losowego przydzielania poświadczeń konta administratora lokalnego przy użyciu usługi Active Directory. Ograniczona pomoc administratora hasła (LAPA) nie istnieje. Nessus to skaner luk w zabezpieczeniach, a Metasploit to platforma eksploatacyjna wykorzystywana do uruchamiania i atakowania sieci.

73. D. Streszczenie wykonawcze nie powinno zawierać szczegółów technicznych. Streszczenie to najważniejsza część raportu. Powinien być napisany w sposób, który przekazuje wszystkie ważne wnioski z raportu w jasny sposób, który jest napisany w terminach laika. Tester powinien wyjaśnić, co zostało odkryte prostym językiem i opisać ryzyko dla biznesu w sposób zrozumiały dla klienta.

74. B, C i D. CompTIA zwraca uwagę na trzy ważne czynności porządkowe po nawiązaniu kontaktu:

■ Usunięcie wszelkich powłok zainstalowanych w systemach podczas testu penetracyjnego.

■ Usunięcie wszelkich utworzonych przez testerów kont, poświadczeń lub tylnych drzwi, które zostały zainstalowane podczas testowania.

■ Usunięcie wszelkich narzędzi, które zostały zainstalowane podczas testowania. Naprawa luk w zabezpieczeniach jest działaniem następczym i nie jest przeprowadzana w ramach testu. Testerzy powinni usunąć wszelkie powłoki lub inne narzędzia zainstalowane podczas testowania, a także usunąć wszelkie utworzone przez siebie konta lub poświadczenia.

75. D. W tym scenariuszu omawiasz technologię. Kontrole technologiczne zapewniają również skuteczną ochronę przed wieloma zagrożeniami bezpieczeństwa. Istnieją trzy główne kategorie działań naprawczych. Kategorie to ludzie, proces i technologia.

76. B. Lista słów jest poprawną odpowiedzią.

77. A. RMF, Xcode i Clutch nie mają nic wspólnego z debugowaniem urządzeń wbudowanych. JTAG to branżowy standard i powszechny interfejs sprzętowy do weryfikacji projektów i metodologii testowania. Zazwyczaj dodawany (a czasami ukryty) przez producenta interfejs JTAG może być używany do łączenia się z konsolą i uzyskiwania dostępu z wiersza poleceń do wbudowanego urządzenia.

78. B. Wybór D jest nadal prawidłowym sposobem zakończenia procesu, ale nie jest najłatwiejszy, gdy istnieje wiele procesów, więc killall iproxy jest najlepszą opcją.

79. A. Domyślnie Clutch przechowuje wszystkie pliki IPA w katalogu /var/tmp/clutch.

80. B. NSAppTransportSecurity określa zmiany domyślnego zachowania zabezpieczeń połączeń HTTP w aplikacjach iOS i macOS. Zmiana domyślnego zachowania bezpieczeństwa powinna być wykonywana tylko wtedy, gdy potrzebujesz wyjątku od najlepszych praktyk bezpieczeństwa, co może uniemożliwić wprowadzenie aplikacji na rynek w Apple Store.