1. C. Pierwszym krokiem w procesie testów penetracyjnych jest współpraca z klientem w celu jasnego zdefiniowania zakresu testu. Zakres określa, co będą robić testerzy penetracji i jak będą spędzać czas. Badanie produktów organizacji to zadanie, które prawdopodobnie zostanie wykonane po określeniu zakresu prac. Określenie budżetu i uzyskanie autoryzacji to podzadania, które są zwykle wykonywane jako część całego procesu określania zakresu.

2. D. Oceny zespołu czerwonego są zwykle bardziej ukierunkowane niż zwykłe testy penetracyjne. Czerwony zespół działa jak napastnik, atakując wrażliwe dane lub systemy w celu uzyskania dostępu. Oceny oparte na celach lub na celach są zwykle zaprojektowane w celu oceny ogólnego bezpieczeństwa organizacji. Oceny oparte na zgodności mają na celu sprawdzenie zgodności z określonymi przepisami.

3. C. Ponieważ akta pacjentów są chronione przez prawo HIPPA w Stanach Zjednoczonych, jest to przykład oceny zgodności. Oceny oparte na zgodności mają na celu sprawdzenie zgodności z określonymi przepisami. Oceny oparte na celach są zwykle przeznaczone do oceny ogólnego bezpieczeństwa organizacji. Oceny w postaci szarej i białej skrzynki określają poziom wiedzy osoby atakującej na temat organizacji.

4. D. Test białoskrzynkowy jest wykonywany z pełną wiedzą na temat podstawowej technologii, konfiguracji i ustawień sieci organizacji docelowej. W teście czarnoskrzynkowym testerom nie zapewnia się dostępu ani informacji o środowisku docelowym. Oceny oparte na celach lub obiektywnych są zwykle zaprojektowane w celu oceny ogólnego bezpieczeństwa organizacji.

5. A. Test szarej skrzynki może dostarczyć testerom penetracyjnym pewnych informacji o środowisku bez podawania pełnego dostępu, poświadczeń lub szczegółów konfiguracji. Test białoskrzynkowy jest wykonywany z pełną znajomością podstawowej sieci. W teście czarnoskrzynkowym testerom nie zapewnia się dostępu ani informacji o środowisku docelowym. Oceny oparte na zgodności mają na celu sprawdzenie zgodności z określonymi przepisami.

6. B. W tym scenariuszu wymagany jest test penetracyjny w oparciu o czarną skrzynkę, więc prawdopodobnie spędzisz większość czasu na gromadzeniu informacji i identyfikacji podatności na etapie oceny. Dzieje się tak, ponieważ z definicji powinieneś mieć niewielką wiedzę na temat organizacji lub jej sieci przed uruchomieniem testu lub nie mieć jej wcale.

7. B. Polecenie whois może służyć do zbierania informacji z publicznych rejestrów o tym, kto jest właścicielem określonej domeny.

8. A. Polecenie nslookup jest dołączone do większości systemów operacyjnych, w tym Windows i Linux, i może być używane do tłumaczenia nazwy domeny organizacji na skojarzone z nią adresy IP.

9. C. theHarvester to narzędzie dostępne w niektórych dystrybucjach Linuksa, takich jak Kali Linux, którego można używać do wysyłania zapytań do wyszukiwarek w celu znalezienia adresów e-mail, nazwisk pracowników i innych szczegółów dotyczących organizacji docelowej.

10. E. Narzędzie do rozpoznawania zapewnia strukturę rozpoznania sieci, która umożliwia przeprowadzenie rozpoznania organizacji w sieci typu open source. Censys to narzędzie internetowe, które sonduje podany adres IP. Polecenie whois może służyć do zbierania informacji z publicznych rekordów o tym, kto jest właścicielem określonej domeny. Shodan to wyspecjalizowane narzędzie, którego tester penetracyjny może używać do przeszukiwania publicznych źródeł w celu znalezienia dowodów na istnienie urządzenia Internetu rzeczy (IoT), które organizacja docelowa mogła wdrożyć w swojej sieci.

11. A. W tym scenariuszu wykorzystano atak typu phishing, ponieważ złośliwa wiadomość e-mail została wysłana bezkrytycznie do wszystkich pracowników w organizacji.

12. C. W tym scenariuszu wykorzystano atak typu spear phishing, ponieważ złośliwa wiadomość e-mail została spreparowana specjalnie dla określonego pracownika. Z drugiej strony ogólny atak phishingowy zostałby wysłany bezkrytycznie do dużej grupy pracowników w organizacji.

13. D. Atak wielorybniczy jest zasadniczo formą ataku typu spear phishing, który jest skierowany w szczególności do pracowników zarządu, takich jak dyrektor generalny, dyrektor finansowy, dyrektor operacyjny, dyrektor ds. Informatyki i tak dalej. Z drugiej strony standardowy atak typu spear phishing zostałby wysłany do pracownika niższego szczebla w organizacji.

14. B. W tym scenariuszu wykorzystano atak typu „phishing" (nazywany również atakiem smishingowym). Atak smishingowy wykorzystuje wiadomości tekstowe zamiast e-maili do przeprowadzenia ataku phishingowego.

15. B. W tym scenariuszu zastosowano głosowy atak phishingowy (zwany również atakiem vishing). Atak typu vishing wykorzystuje rozmowę telefoniczną zamiast wiadomości e-mail w celu przeprowadzenia ataku phishingowego. Zasadniczo osoba atakująca dzwoni do konkretnego pracownika podszywającego się pod kogoś innego w celu uzyskania informacji.

16. A. Opcja –sS powoduje, że narzędzie nmap przeprowadza skanowanie portu SYN podanego systemu docelowego.

17. D i E. Polecenie nmap 192.168.1.0/24 powoduje, że narzędzie nmap przeskanuje każdy system w podsieci od .1 do .254. Podobnie polecenie nmap 192.168.1.1-254 powoduje, że narzędzie nmap przeskanuje każdy system w podsieci, od .1 do .254.

18. A i B. Polecenie nmap 192.168.1.1 -sS powoduje, że narzędzie nmap przeprowadza skanowanie portu SYN określonego systemu docelowego. Podobnie polecenie nmap 192.168.1.1 powoduje również, że narzędzie nmap przeprowadza skanowanie portu SYN określonego systemu docelowego, ponieważ skanowanie SYN jest używane domyślnie, jeśli nie określono innego typu skanowania.

19. D. Polecenie nmap 192.168.1.1 -O powoduje, że narzędzie nmap używa odcisków palców stosu TCP / IP do określenia systemu operacyjnego zainstalowanego na zdalnym hoście.

20. A. Polecenie nmap 192.168.1.1 -A umożliwia wykrywanie systemu operacyjnego, wykrywanie wersji usługi, skanowanie skryptów i śledzenie trasy do zdalnego hosta.

21. B. Kiedy normalizujesz dane z testu penetracyjnego, agregujesz wszystkie dane wygenerowane przez wszystkie różne narzędzia i procesy użyte podczas testu i formatujesz je w taki sposób, aby były spójne i skorelowane. Celem jest sprawienie, aby klient mógł odczytać zagregowane dane i zrozumieć, co i kiedy wydarzyło się podczas testu.

22. D. Raport końcowy, który piszesz do testu penetracyjnego, powinien zawierać sekcję zatytułowaną Metodologia. W tej sekcji opisujesz metodologię testów penetracyjnych użytą do przeprowadzenia testu. W tym scenariuszu byłoby to odpowiednie miejsce do wskazania, że do przeprowadzenia testu zastosowano standard PCI DSS.

23. A. Termin świadomość sytuacyjna odnosi się między innymi do stanu wspólnego zrozumienia między klientem a testerem stanu bezpieczeństwa sieci klienta.

24. C. Termin dekonflikt odnosi się do procesu komunikacji między klientem a testerem w celu ustalenia, czy atak wykryty podczas testu penetracyjnego pochodzi od autoryzowanego testera penetracyjnego, czy też jest to prawdziwy atak zainicjowany przez osobę trzecią. haker imprezowy.

25. B. Termin deeskalacja odnosi się do procesu komunikowania się między klientem a testerem w celu zaprzestania exploitów wykorzystywanych podczas testu penetracyjnego z powodu negatywnych skutków, jakie mogą one mieć w sieci.

26. D. W ocenie łańcucha dostaw przeprowadza się test penetracyjny na dostawcach organizacji, aby upewnić się, że ich sieci są bezpieczne i nie mogą być wykorzystywane jako punkt zwrotny do narażenia samej organizacji. Ocena oparta na celach ma na celu przetestowanie określonego aspektu bezpieczeństwa organizacji. Test poprzedzający połączenie jest zwykle przeprowadzany na organizacji przed połączeniem z inną.

27. D. Ocena zespołu czerwonego jest zwykle przeprowadzana przez testerów wewnętrznych, aby upewnić się, że personel IT organizacji (zespół niebieski) jest w stanie odpowiednio obronić sieć. Ocena oparta na celach ma na celu przetestowanie określonego aspektu bezpieczeństwa organizacji. Test łańcucha dostaw obejmuje testowanie dostawców organizacji. Test zgodności jest przeprowadzany w celu zapewnienia, że organizacja zachowuje zgodność z przepisami rządowymi lub politykami korporacyjnymi.

28. A. Ogólnie rzecz biorąc, gdybyś uszeregował cyberprzestępców na poziomy od najmniej groźnego do najbardziej groźnego, wyglądałoby to mniej więcej tak: script kiddie > haktywista > złośliwy insider > zorganizowana przestępczość > państwo narodowe.

29. C. To jest przykład modelowania zagrożeń. Korzystając z modelowania zagrożeń, określasz rodzaj zagrożenia, które chcesz emulować podczas testu penetracyjnego. Następnie używasz tych samych narzędzi, technik i podejść, których zwykle używałby typ zagrożenia.

30. A. To jest przykład akceptacji ryzyka. Oceniłeś tolerancję klienta na wpływ, jaki test penetracyjny może wywrzeć na organizację. Ważne jest, aby klient był gotowy i zdolny do zaakceptowania faktu, że test penetracyjny może spowodować awarię sieci lub zakłócenie usług.

31. A. Narzędzie sslyze to narzędzie do testowania penetracji, które jest powszechnie używane do przeprowadzania inspekcji certyfikatów.

32. B i C. Dane wyjściowe komendy sslyze w tym przykładzie pokazują, że serwer WWW odpowiedział na zapytania TLSv1.1 i TLSv1.2, ale nie odpowiedział na zapytania SSLv2, SSLv3 lub TLSv1.

33. A i C. Możesz użyć tcpdump lub Wireshark do przechwytywania pakietów w sieci przewodowej. Z tych dwóch Wireshark jest zwykle uważany za najbardziej przyjazny dla użytkownika interfejs.

34. A. Narzędzie Aircrack-ng może być używane do wykrywania sieci bezprzewodowych w zasięgu, a następnie złamania ich szyfrowania. Proces ten jest bardzo szybki w przypadku starych sieci WEP, trudniejszy, ale wykonalny w przypadku sieci WPA i dość trudny w przypadku sieci WPA2.

35. A. Zanim interfejs sieci bezprzewodowej będzie mógł być używany do przechwytywania ruchu w sieci bezprzewodowej, musi być skonfigurowany do działania w trybie monitorowania na określonym kanale używanym przez punkt dostępu do transmisji.

36. B. Obejście zamka ma miejsce, gdy atakujący uniemożliwia działanie mechanizmu blokującego drzwi. W tym przykładzie dokonano tego poprzez umieszczenie drewnianego klina w ościeżnicy drzwi, zapobiegając całkowitemu zamknięciu drzwi i blokowaniu mechanizmu blokującego.

37. A. Większość automatycznie zamykanych systemów drzwiowych ma pewien rodzaj mechanizmu awaryjnego otwierania w razie awarii. Ideą tego jest to, że w przypadku jakiegoś zagrożenia, takiego jak pożar, drzwi muszą zostać automatycznie odblokowane, aby zapobiec uwięzieniu ludzi w środku lub uniemożliwieniu wejścia personelowi ratunkowemu. Jeśli wiesz, jaki mechanizm awaryjnego otwierania jest używany, możesz być w stanie ręcznie uruchomić go, aby otworzyć zamknięte drzwi.

38. B i D. W tym scenariuszu do odnalezienia odrzuconej odznaki dostępu użyto nurkowania w śmietniku. Następnie klonowanie odznak zostało użyte do stworzenia fałszywej odznaki.

39. D. Klonowanie identyfikatora ma miejsce, gdy atakujący wykonuje kopię ważnej karty dostępu, aby wejść do obiektu. Kopiując podpis RFID ważnej karty, tester penetracyjny w tym scenariuszu może użyć fałszywej karty, aby uzyskać dostęp do obiektu organizacji docelowej przy użyciu poświadczeń upoważnionego pracownika. Ponieważ starannie wybrał odznakę pracownika wysokiego szczebla do klonowania, może on mieć dostęp do bardziej wrażliwych obszarów obiektu.

40. A. NetBIOS to protokół transportowy używany przez systemy Windows do udostępniania zasobów, takich jak foldery współdzielone lub drukarki. Gdy atakujący zidentyfikuje, że port 139 jest otwarty na urządzeniu, NBTSTAT może zostać użyty do umieszczenia urządzenia. Na przykład możesz odkryć nazwę komputera urządzenia i określić, czy jest to stacja robocza, czy serwer. Wszystkie te informacje można zebrać bez jakiegokolwiek uwierzytelnienia.

41. A i D. Narzędzia whois i nslookup mogą być wykorzystane do biernego prowadzenia rekonesansu w organizacji docelowej. Ponieważ przekazują informacje, które są dostępne dla ogółu społeczeństwa, jest mało prawdopodobne, aby korzystanie z tych narzędzi wzbudziło jakiekolwiek podejrzenia.

42. B i C. Narzędzia nmap i hping mogą być używane do aktywnego wyliczania i odcisku palca systemów docelowych.

43. A i B. John the Ripper, a także Cain i Abel mogą być wykorzystywane do łamania haseł z offline bazy danych kont użytkowników, takich jak pliki shadow i passwd z systemu Linux.

44. D i E. OWASP ZAP oraz Nessus mogą być używane do skanowania celu w poszukiwaniu luk.

45. B. SQLmap można użyć do brutalnego złamania hasła do bazy danych SQL.

46. B. Zatrudnianie dodatkowych pracowników IT, którzy mają doświadczenie z cyberbezpieczeństwem, jest przykładem strategii łagodzenia opartej na ludziach.

47. C. Zakaz korzystania przez pracowników z zewnętrznych usług w chmurze, takich jak Dysk Google, jest przykładem strategii łagodzenia opartej na procesach.

48. A. Wdrożenie pułapki na człowieka przy wejściu głównym jest przykładem strategii łagodzenia skutków technologii.

49. A. Wdrażanie kierunkowych anten bezprzewodowych i manipulowanie poziomami mocy punktów dostępowych w celu zapobiegania emanacji sygnału to przykłady technologicznych strategii łagodzenia.

50. C. Wymaganie wielokrotnych podpisów przy wypłatach jest przykładem strategii łagodzenia opartej na procesach.

51. A i E. Wykorzystywanie wewnętrznych zespołów do przeprowadzania testów penetracyjnych przynosi dwie główne korzyści. Po pierwsze, posiadają kontekstową wiedzę o organizacji, która może poprawić skuteczność testów. Po drugie, przeprowadzanie testów z wykorzystaniem pracowników

wewnętrznych jest zwykle tańsze niż zatrudnienie wykonawcy testów penetracyjnych. Gdy personel wewnętrzny nie jest zaangażowany w test penetracyjny, może pracować nad innymi projektami dla organizacji.

52. B i C. Zewnętrzne zespoły testów penetracyjnych są zatrudniane w celu przeprowadzenia testów penetracyjnych. Ponieważ nie są bezpośrednio zatrudnieni przez organizację, mają zwykle wyższy stopień niezależności. Nie muszą się martwić, że zdenerwują menedżera lub dyrektora, jeśli zostaną wykryte luki. W rzeczywistości zazwyczaj zachwycają się takim wydarzeniem. Ponadto są one mniej stronnicze, ponieważ nie uczestniczą w projektowaniu ani bieżącym utrzymaniu infrastruktury sieciowej organizacji.

53. C i D. Wewnętrzny zespół ds. testów penetracyjnych może być zbyt blisko związany z organizacją. Na przykład mogą się obawiać, że podatność wykryta podczas testu penetracyjnego może źle odbić się na ich zespole, ponieważ prawdopodobnie zaprojektowali i nadal utrzymują testowaną sieć. Mogłoby to spowodować brak obiektywizmu podczas przeprowadzania testów penetracyjnych.

54. A i C. Korzystanie z zewnętrznego zespołu wykonawców do przeprowadzania testów penetracyjnych ma kilka wad, które należy wziąć pod uwagę. Po pierwsze, może istnieć potencjalny konflikt interesów, jeśli przeprowadzają również testy penetracyjne dla jednego z twoich konkurentów. Po drugie, są dość drogie.

55. C. Testery penetracyjne muszą przyjąć inne podejście w swoim myśleniu. Zamiast próbować bronić się przed wszystkimi możliwymi zagrożeniami, wystarczy znaleźć pojedynczą lukę, którą mogą wykorzystać, aby osiągnąć swoje cele. Aby znaleźć te luki, muszą myśleć jak przeciwnik, który może zaatakować system w prawdziwym świecie. Takie podejście jest powszechnie znane jako przyjęcie nastawienia hakerskiego.

56. C. Ponieważ serwer jest uważany za delikatny system, należy ograniczyć przepustowość wykorzystywaną przez skanowanie luk w zabezpieczeniach. Jeśli tego nie zrobisz, możesz z łatwością wykorzystać wszystkie zasoby serwera za pomocą skanowania i nie pozostawić ich na krytyczne operacje biznesowe. Możesz użyć opcji -Tn z poleceniem nmap, aby ograniczyć skanowanie. W tym scenariuszu powinieneś rozważyć użycie opcji -T2 lub nawet opcji -T1 z poleceniem nmap. Opcja -T0 prawdopodobnie ograniczyłaby skanowanie zbyt mocno, przez co jego ukończenie zajęłoby zbyt dużo czasu.

57. A i E. Kontener może służyć do tworzenia izolowanego środowiska, podobnie jak maszyna wirtualna. W rezultacie wszelkie aplikacje działające w środowisku kontenera mogą nie być wykrywane przez tradycyjne skanowanie luk w zabezpieczeniach. W przeciwieństwie do maszyny wirtualnej kontener współużytkuje większość podstawowego systemu operacyjnego z hostem kontenera. Dlatego luki związane z podstawowym systemem operacyjnym hosta kontenera mogą być dziedziczone przez jego kontenery.

58. A. Statyczna analiza kodu jest przeprowadzana poprzez analizę kodu źródłowego aplikacji. Oczywiście tego typu testy są zwykle wykonywane tylko podczas testu penetracyjnego białej skrzynki. Analiza kodu statycznego nie obejmuje faktycznego uruchamiania programu. Zamiast tego koncentruje się na analizie sposobu napisania aplikacji.

59. B i C. Dynamiczna analiza kodu oraz testy fuzz są wykonywane na uruchomionym kodzie. Ponieważ kod źródłowy nie jest wymagany do przeprowadzenia tych testów, można je wykonać podczas testów penetracyjnych szarej lub czarnej skrzynki.

60. B. Testowanie rozmyte polega na wysyłaniu losowych, nieoczekiwanych lub nieprawidłowych danych do wejść aplikacji w celu sprawdzenia, jak obsługuje te dane. Nazywa się to obsługą wyjątków. Można wdrożyć wiele ataków, które wykorzystują niezdolność aplikacji do prawidłowego obsługiwania nieoczekiwanych danych.

61. B. W przypadku powtarzającego się ataku, tester penetracyjny przechwytuje sygnał radiowy sieci bezprzewodowej docelowej organizacji i ponownie emituje go z dużym wzmocnieniem, aby rozszerzyć jego zasięg. W tym scenariuszu tester penetracyjny może teraz uzyskać dostęp do sieci bezprzewodowej organizacji z parkingu.

62. A. To jest przykład ataku typu SQL injection. Zamiast wpisywać hasło w polu Hasło, tester wstawia instrukcję SQL. Jeśli aplikacja internetowa w tym przykładzie byłaby źle napisana, możliwe, że wyciągnęłaby nazwy użytkowników i hasła dla każdego użytkownika w hipotetycznej bazie danych. Instrukcja UNION SELECT służy do łączenia dwóch niepowiązanych zapytań SELECT w celu pobrania danych z różnych tabel bazy danych. Dobrze napisana aplikacja użyje sprawdzania poprawności danych wejściowych, aby zapobiec przesyłaniu instrukcji SQL w formularzu użytkownika. Te same zasady dotyczą ataków wstrzykiwania HTML, wstrzykiwania poleceń i wstrzykiwania kodu.

63. A. Jest to przykład ataku brutalnego wymuszającego uwierzytelnienie. W prawdziwym ataku bruteforce wszystkie możliwe kombinacje liter, cyfr i znaków specjalnych będą wypróbowywane jedna po drugiej, dopóki nie zostanie znaleziona właściwa. Jednak tworzenie listy prawdopodobnych haseł w oparciu o osobiste zainteresowania użytkownika znacznie zwiększa prawdopodobieństwo sukcesu.

64. B. To jest przykład przejmowania sesji. Tester był w stanie wykorzystać klucz sesji (plik cookie), aby uzyskać dostęp do sesji użytkownika. Tego typu exploita można wykorzystać w aplikacjach internetowych, w których do utrzymania sesji używany jest plik cookie HTTP. Mimo że witryna mogła używać protokołu TLS/SSL do szyfrowania danych uwierzytelniających, plik cookie sesji często nie jest szyfrowany. Jeśli zostanie przechwycony, tester może przejąć sesję użytkownika.

65. C. Jest to przykład ataku przekierowującego, ponieważ użytkownicy są przekierowywani na fałszywą stronę internetową przez wiadomości phishingowe.

66. A. Tworząc tablicę asocjacyjną w skrypcie Bash, używasz następującej składni: nazwa_tablicy[nazwa_elementu] = wartość. W tym przykładzie wiersz Target[HostName] = FS1 przypisuje wartość FS1 do elementu o nazwie HostName w tablicy Target.

67. D. Tworząc tablicę asocjacyjną w skrypcie Rubiego, używasz następującej składni: _nazwa_tablicy = {"nazwa_elementu" => "wartość"} . W tym przykładzie wiersz _Target = {"HostName" => "FS1"} przypisuje wartość FS1 do elementu o nazwie HostName w tablicy Target.

68. C. Podczas tworzenia tablicy asocjacyjnej w skrypcie PowerShell używasz następującej składni: $array_name.element_name = "value" . W tym przykładzie wiersz $Target.HostName = 'FS1' przypisuje wartość FS1 do elementu o nazwie HostName w tablicy Target.

69. B. Tworząc tablicę asocjacyjną w skrypcie PowerShell, użyj następującej składni: array_name = [{"element_name":"wartość"}]. W tym przykładzie wiersz Target = [{"HostName":"FS1"}] przypisuje wartość FS1 do elementu o nazwie HostName w tablicy Target.

70. B. Porównując dwie wartości w skrypcie Rubiego, aby sprawdzić, czy są one równe, używasz operatora relacyjnego ==.

71. D. Protokół Telnet nie wykorzystuje szyfrowania do ochrony transmisji sieciowych, co oznacza, że dane uwierzytelniające do zdalnego systemu oraz przesyłane dane są przesyłane jako zwykły tekst. Aby

temu zaradzić, zaleca się, aby klient używał serwera Secure Shell (SSH) i klienta do zdalnego dostępu do serwera. SSH szyfruje informacje uwierzytelniające, a także transfery danych między systemami.

72. A. Narzędzie rcp nie używa szyfrowania do ochrony transmisji sieciowych, co oznacza, że dane uwierzytelniające do zdalnego systemu oraz przesyłane dane są wysyłane jako zwykły tekst. Aby temu zaradzić, zaleca się, aby klient używał polecenia scp do kopiowania plików między serwerami. Narzędzie scp jest częścią pakietu narzędzi SSH, który szyfruje informacje uwierzytelniające oraz transfery danych między systemami.

73. B. W tym scenariuszu sieć bezprzewodową można wzmocnić, zmieniając domyślną nazwę użytkownika i hasło administratora na kontrolerze bezprzewodowym. Listy domyślnych nazw użytkowników i haseł są łatwo dostępne w Internecie i nie należy ich używać.

74. A i B. W tym scenariuszu sieć bezprzewodową można wzmocnić, wdrażając filtrowanie adresów MAC. Zapewnia to podstawową warstwę ochrony, uniemożliwiając nieautoryzowanym systemom łączenie się z siecią bezprzewodową. Jednak adresy MAC można łatwo sfałszować po zidentyfikowaniu znanego dobrego adresu. Tak więc sieć bezprzewodową można dodatkowo wzmocnić, wdrażając uwierzytelnianie 802.1x. Eliminuje to słabość związaną ze wstępnie udostępnionymi kluczami poprzez zaimplementowanie oddzielnego serwera uwierzytelniania (takiego jak serwer RADIUS).

75. A i D. W tym scenariuszu sieć bezprzewodową można wzmocnić za pomocą kierunkowych punktów dostępu. Pomoże to zapobiec przedostawaniu się sygnału na parking. Ponadto w sieci bezprzewodowej należy wyłączyć DHCP. Chociaż sprawia to, że administracja jest znacznie trudniejsza, uniemożliwia także atakującym, którzy naruszają sieć bezprzewodową, automatyczne otrzymywanie wszystkich informacji konfiguracyjnych, których potrzebują, aby uzyskać dostęp do zasobów sieciowych.

76. C. NFSv3 i starsze wersje mapują numeryczne identyfikatory UID i GID na pliki i katalogi w systemie plików NFS. Podczas montowania udziału NFS z klienta korzystającego z NFSv3 zamiast nazwy użytkownika lub grupy może pojawić się UID lub GID, ponieważ lokalny system operacyjny nie może na nie mapować, ponieważ nie znajdujesz się w domenie (np. LDAP). lub użytkownik nie istnieje.

77. A, B, C. Otwarte serwery przekazujące pocztę skonfigurowane do dostępu anonimowego mogą umożliwić atakującemu podszywanie się pod zarówno wewnętrzny, jak i zewnętrzny adres docelowy. Polecenie VRFY służy do poproszenia serwera o informacje o adresie, a EXPN służy do poproszenia serwera o członkostwo na liście dyskusyjnej. Jeśli polecenie VRFY skierowane na adres konta lokalnego zakończy się pomyślnie, może to umożliwić osobie atakującej wyliczenie kont użytkowników lokalnych. Jeśli polecenie EXPN powiedzie się, serwer pokaże każdego subskrybenta listy mailingowej. Informacje te mogą pomóc napastnikowi w przyszłych kampaniach phishingu typu spear.

78. A. Atak Karma będzie skierowany na każdy wykryty SSID w celu zwiększenia prawdopodobieństwa wykorzystania.

79. C. L2PING zapewnia metodę, która może być używana do identyfikacji urządzeń Bluetooth, a także nakierowania ich na ataki DoS przy użyciu docelowego adresu MAC.

80. D. TC2 nie jest prawidłową warstwą stosu protokołów Bluetooth. Specyfikacja protokołu sterowania telefonią (TCS) jest jednak ważną warstwą w stosie protokołów i służy do sterowania funkcjami telefonicznymi w urządzeniu mobilnym.