1. B. Ponieważ tester do przeprowadzenia testu używa wewnętrznego konta e-mail (takiego, jakiego używa typowy pracownik), tester najprawdopodobniej przeprowadza test szarej skrzynki. W teście czarnej skrzynki tester musiałby użyć zewnętrznego konta e-mail. W teście białej skrzynki tester prawdopodobnie użyje podwyższonych uprawnień i dostępu do przeprowadzenia testu.

2. B. Ponieważ tester ma szeroki wewnętrzny dostęp do sieci docelowej, test białej skrzynki zwykle zapewnia najbardziej wyczerpującą ocenę. Można poświęcić więcej czasu na badanie głębokich luk w zabezpieczeniach niż w przypadku testu czarnej lub szarej skrzynki.

3. A i B. Zakres tego zaangażowania w tym scenariuszu jest ograniczony do wewnętrznej infrastruktury sieciowej. Microsoft Office 365, Google Docs i Microsoft Azure to wszystkie usługi oparte na chmurze hostowane przez strony trzecie i dlatego są uważane za nieobjęte zakresem.

4. A. Najważniejszym krokiem w procesie planowania i określania zakresu testów penetracyjnych jest uzyskanie pisemnej zgody osoby docelowej na wykonanie testu. Bez pisemnej zgody jesteś uważany za hakera i podlegasz federalnym, stanowym i lokalnym przepisom dotyczącym przestępczości komputerowej (takim jak Kodeks Stanów Zjednoczonych, tytuł 18, rozdział 47, sekcje 1029 i 1030).

5. C. Świadectwo pracy (SOW) to formalny dokument określający zakres testu penetracyjnego. Określa dokładnie, co wydarzy się podczas testu. MSA określa warunki, które będą regulować przyszłe umowy. Umowa o zachowaniu poufności określa, co każda ze stron umowy może ujawnić stronom trzecim. Zamówienie zakupu to wiążąca umowa zakupu od dostawcy.

6. D. W tym przykładzie dane wyjściowe informują nas, że serwer poczty e-mail odpowiada na polecenia SMTP HELO. Przydatne informacje można czasem uzyskać z serwera poczty e-mail za pomocą poleceń HELO.

7. A i D. Proces wyliczania obejmuje łączenie się z każdym hostem wykrytym w segmencie sieci i identyfikowanie kluczowych informacji, w tym usług uruchomionych na każdym hoście oraz numeru wersji zainstalowanego systemu operacyjnego.

8. D. Proces wyliczania obejmuje połączenie z każdym hostem odkryte w segmencie sieci i identyfikujące kluczowe informacje. W tym przykładzie zwróć uwagę, że klasa systemu operacyjnego urządzenia jest następująca:

Typ: WAP

Dostawca: Belkin

Rodzina systemów operacyjnych: wbudowana

Z tych informacji można rozsądnie wywnioskować, że to urządzenie jest bezprzewodowym punktem dostępowym.

9. B. W sekcji Używane porty zwróć uwagę, że port 80 TCP jest otwarty na urządzeniu. Oznacza to, że najprawdopodobniej działa serwer WWW HTTP.

10. A. Wyszukując w Internecie numer wersji systemu operacyjnego wyświetlany w obszarze System operacyjny, prawdopodobnie można wykryć domyślną nazwę użytkownika i hasło administratora używane przez urządzenie. Kilka głośnych exploitów w ciągu ostatnich kilku lat zostało ułatwionych dzięki temu, że implementator systemu nie zmienił domyślnej nazwy użytkownika i hasła używanych przez urządzenia infrastruktury sieciowej.

11. B. Większość ludzi zareaguje na prośbę o podjęcie działania, jeśli będą obawiać się konsekwencji zaniechania działania. To jedna z najbardziej podstawowych ludzkich motywacji.

12. A. Piggybacking ma miejsce, gdy intruz przechodzi wraz z upoważnioną osobą przez fizyczną barierę, taką jak zamykane drzwi lub kołowrót. Dzieje się to bez wiedzy i zgody osoby uprawnionej.

13. B. Tailgating ma miejsce, gdy intruz przechodzi wraz z upoważnioną osobą przez fizyczną barierę, taką jak zamykane drzwi lub kołowrót. Dzieje się to za wiedzą i/lub zgodą osoby upoważnionej.

14. A. Piggybacking ma miejsce, gdy intruz wraz z jedną lub kilkoma upoważnionymi osobami przechodzi przez fizyczną barierę, taką jak zamykane drzwi lub kołowrót. Dzieje się to bez wiedzy i zgody osoby uprawnionej.

15. D. Skakanie przez ogrodzenie ma miejsce, gdy osoba nieupoważniona po prostu przeskakuje przez fizyczną barierę mającą na celu kontrolę dostępu. W tym scenariuszu tester penetracyjny po prostu przechodzi nad bramką obrotową, która ma zapobiegać wejściu nieuprawnionych osób.

16. A. Opcja –f powoduje, że nmap skanuje przy użyciu małych, pofragmentowanych pakietów. Czasami te małe pakiety mogą być trudniejsze do prawidłowego przeanalizowania przez zapory filtrujące pakiety.

17. B. Opcja –D powoduje, że nmap wysyła skany ze sfałszowanego adresu IP. Za pomocą tej opcji możesz określić jeden lub więcej fałszywych źródłowych adresów IP.

18. D. Opcja –iR powoduje, że nmap skanuje określoną liczbę losowych hostów. Na przykład, jeśli chcesz przeskanować 50 losowych hostów, użyj opcji –iR 50 z poleceniem nmap.

19. C. Opcja –F powoduje, że nmap skanuje host o określonej liczbie w poszukiwaniu 100 najczęściej używanych portów IP. Na przykład to skanowanie obejmowałoby porty 20, 21, 23, 25, 53, 80 i tak dalej. Czasami nazywa się to szybkim skanowaniem portów.

20. A. Opcja --proxy powoduje, że nmap przekazuje połączenia przez serwer proxy. Ta opcja wymaga podania adresu IP jednego lub więcej serwerów proxy.

21. E. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś zgłosić swoje zalecenia w sekcji Podsumowanie, w tym, kiedy uważasz, że klient powinien przeprowadzić kolejne testy penetracyjne.

22. D. Zazwyczaj nie ma prawnie wymaganego czasu przechowywania raportów po zakończeniu testu penetracyjnego. Ilość czasu, przez którą będziesz musiał przechowywać raport klienta, będzie zwykle regulowana umową z klientem.

23. D. Pisemne sprawozdanie z ustaleń zawiera bardzo wrażliwe informacje i dlatego powinno się z nim obchodzić w bezpieczny sposób. Nie należy go przechowywać w sposób, który pozwalałby na jego łatwą kradzież. W tym scenariuszu przechowywanie raportu w zaszyfrowanym pliku na serwerze plików utrudniłoby kradzież pliku niż inne wymienione opcje.

24. A. Pisemne sprawozdanie z ustaleń zawiera bardzo wrażliwe informacje i dlatego powinno się z nim obchodzić w bezpieczny sposób. Nie należy go przechowywać w sposób, który pozwalałby na jego łatwą kradzież. W tym scenariuszu przechowywanie papierowej kopii raportu w zamkniętej szafce na dokumenty, która została przykręcona do podłogi, utrudniłoby kradzież raportu niż inne wymienione opcje.

25. A. Pisemne sprawozdanie z ustaleń zawiera bardzo wrażliwe informacje i dlatego powinno się z nim obchodzić w bezpieczny sposób. Nie należy go przechowywać w sposób, który pozwalałby na jego łatwą kradzież. W tym scenariuszu nagranie pliku na dysk optyczny i przechowywanie go w zabezpieczonym sejfie utrudniłoby kradzież raportu niż inne wymienione opcje.

26. A. Payment Card Industry Data Security Standard (PCI-DSS) to zestaw zabezpieczeń, które firmy muszą wdrożyć w celu ochrony danych kart kredytowych. Na przykład jedno z wymagań określa, że oprogramowanie antywirusowe ma być zainstalowane we wszystkich systemach i musi być regularnie aktualizowane.

27. A. Payment Card Industry Data Security Standard (PCI-DSS) to zestaw zabezpieczeń, które firmy muszą wdrożyć w celu ochrony danych kart kredytowych. Na przykład jedno z wymagań określa, że w organizacji obowiązuje polityka silnych haseł.

28. A i D. Payment Card Industry Data Security Standard (PCI-DSS) to zestaw zabezpieczeń, które firmy muszą wdrożyć w celu ochrony danych kart kredytowych. Na przykład dwa z wymagań określają, że organizacja musi monitorować i kontrolować wszelki dostęp do danych posiadaczy kart oraz że dostęp do tych danych musi być ograniczony na zasadzie niezbędnej wiedzy.

29. A. Ustawa Gramm-Leach-Bliley (GLBA) reguluje, w jaki sposób instytucje obsługują dane osobowe klientów. Na przykład wymaga od firm posiadania pisemnego planu bezpieczeństwa informacji, który identyfikuje procesy i procedury mające na celu ochronę tych informacji.

30. C. Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych z 1996 r. reguluje organizacje opieki zdrowotnej. Muszą być zgodne z zasadami i przepisami określonymi w ustawie, takimi jak wymaganie analizy ryzyka i testowanie mechanizmów bezpieczeństwa w organizacji. .

31. C. Skanowanie ukrywające zlicza hosty w sieci docelowej poprzez manipulowanie trójstronnym uzgadnianiem TCP. Najpierw wysyła do celu pakiet SYN. Jeśli zostanie odebrany pakiet SYN-ACK, skaner wie, że host docelowy istnieje. SYN-ACK zawiera również ograniczoną ilość informacji o hoście, które mogą zostać przechwycone i przeanalizowane przez skaner.

32. D. Skanowanie stealth zlicza hosty w sieci docelowej poprzez manipulowanie uzgadnianiem trójstronnym TCP. Najpierw wysyła do celu pakiet SYN. Jeśli zostanie odebrany pakiet SYN-ACK, skaner wie, że host docelowy istnieje. Zamiast zakończyć połączenie, wysyłając do celu pakiet ACK, host skanujący resetuje połączenie, wysyłając pakiet RST.

33. A. Skany Stealth nie są obecnie uważane za tak dyskretne, jak kiedyś. Większość nowoczesnych urządzeń IDS/IPS może wykryć niezwykle wysoką częstotliwość pakietów RST w sieci utworzonych podczas skanowania stealth i podjąć odpowiednie działania. Na przykład IDS może wygenerować alert. IPS może generować alert, a także blokować ruch z hosta skanującego.

34. B. Ponieważ pełne połączenia są ustanawiane z każdym hostem podczas pełnego skanowania podatności, można je dokładnie przesłuchać i pobrać odcisk palca. W rezultacie pełny skan zwykle daje najdokładniejsze informacje. Jednak są też najłatwiejsze do wykrycia przez obrońców.

35. D. Skanowanie podatności na zgodność jest wykorzystywane do weryfikacji, czy organizacja docelowa spełnia wymagania danego prawa lub polityki. W tym przykładzie test penetracji PCI-DSS zwykle wymaga skanowania podatności na zgodność z PCI-DSS .

36. B. Zalewając router fałszywym ruchem ICMP, tester utrudnia routerowi obsługę uzasadnionych żądań sieciowych. Ponieważ do przeprowadzenia testu warunków skrajnych użyto wielu hostów, jest to przykład standardowego ataku typu rozproszona odmowa usługi (DDoS).

37. A. Systemy kontroli dostępu do sieci (NAC) wymagają, aby hosty sieciowe spełniały wymagania polityki bezpieczeństwa przed uzyskaniem dostępu do sieci, nawet jeśli zostały prawidłowo podłączone do gniazda sieciowego lub skojarzone z punktem dostępu. Nieautoryzowane lub w złej kondycji urządzenia są zwykle umieszczane w izolowanej sieci naprawczej do czasu uzyskania autoryzacji lub zapewnienia zgodności. Po wykonaniu tej czynności mogą połączyć się z rzeczywistym segmentem sieci.

38. B. Jednym ze sposobów przeprowadzenia exploita obejścia NAC jest sfałszowanie systemu testera za pomocą adresu MAC autoryzowanego urządzenia. Dopóki system testera spełnia wymagania polityki bezpieczeństwa organizacji, system NAC powinien umożliwiać mu dostęp do sieci produkcyjnej.

39. D i E. Telefony VoIP i urządzenia SCADA zazwyczaj nie mogą być konfigurowane w sposób umożliwiający im spełnienie polityki bezpieczeństwa i wymagania systemu NAC. Na przykład zazwyczaj nie można zainstalować oprogramowania antymalware na telefonie VoIP lub urządzeniu SCADA. Dlatego też systemy te są często umieszczane na białej liście w implementacjach NAC, co pozwala im ominąć wymagania stosowane w innych systemach. .

40. A. Podwójne tagowanie tagów VLAN jest dozwolone w specyfikacji 802.1q. Umożliwia to hostowi „przeskakiwanie” między sieciami VLAN.

41. D. Narzędzie searchsploit to narzędzie wyszukiwania z wiersza poleceń, które służy do przeszukiwania bazy danych online Exploit-DB pod kątem znanych exploitów.

42. D. Narzędzie responder może być używane do przeprowadzania zatruwania LLMNR i NBT-NS, potencjalnie umożliwiając testerowi penetracji przekierowanie klientów do jej laptopa i przechwycenie ich poświadczeń w postaci nazw użytkowników i zaszyfrowanych haseł.

43. C. Narzędzie do testowania penetracji imppacket składa się ze zbioru klas Pythona używanych do niskopoziomowego dostępu do protokołów sieciowych, takich jak protokoły SMB i MSRPC.

44. A. Narzędzie do testowania penetracji Metasploit Framework (MSF) zapewnia ogromną liczbę exploitów, które można wykorzystać do włamania się do sieci organizacji docelowej.

45. B i D. Podczas deklarowania zmiennej zarówno Bash, jak i Python używają tej samej składni: nazwa_zmiennej = wartość.

46. A. Każda usługa sieciowa włączona na serwerze rozszerza obszar ataku tego serwera. Dlatego należy instalować tylko te usługi, które są rzeczywiście potrzebne. W tym scenariuszu serwer sieciowy prawdopodobnie nie wymaga działania usług DNS, DHCP, drukowania ani poczty e-mail. Powinny one zostać usunięte.

47. B i D. Każda usługa sieciowa włączona na serwerze rozszerza obszar ataku tego serwera. Dlatego należy instalować tylko te usługi, które są rzeczywiście potrzebne. W tym scenariuszu kontroler domeny nie powinien obsługiwać funkcji Hyper-V, która jest używana do wirtualizacji. Podobnie Usługi federacyjne są używane tylko w sytuacjach, gdy jedna domena usługi Active Directory jest połączona z („federacją”) z inną domeną usługi Active Directory.

48. A i E. Aby wzmocnić konta użytkowników w systemach komputerowych z systemem Windows, należy skonfigurować blokadę konta za pomocą zasad grupy. Pomoże to spowolnić, a nawet zapobiec atakom typu brute-force lub zgadywania haseł. Należy również natychmiast wyłączyć lub usunąć wszystkie nieużywane konta użytkowników.

49. B i D. Aby wzmocnić konta użytkowników w systemie komputerowym z systemem Windows, należy użyć zasad grupy, aby wymusić wymagania dotyczące złożoności hasła. Na przykład możesz wymagać określonej długości hasła i zawierać określone kombinacje znaków. Należy również użyć zasad grupy, aby wymusić wymagania dotyczące starzenia się haseł. Wymaga to od użytkowników regularnej zmiany haseł.

50. E. Aby wzmocnić komunikację sieciową w systemie komputerowym z systemem Windows, należy ograniczyć dostęp do komputera przez sieć tylko do uwierzytelnionych użytkowników.

51. B. Test szarej skrzynki jest czasami określany jako częściowa ocena wiedzy, ponieważ testerzy penetracji mają pewną wiedzę o sieci klienta, ale nie mają pełnego obrazu. Ten rodzaj oceny najlepiej naśladuje rzeczywisty atak z wykorzystaniem informacji poufnych.

52. C. Test białej skrzynki jest czasami określany jako pełna ocena wiedzy, ponieważ testerzy penetracji mają pełną wiedzę o sieci klienta, w tym o dostępie administracyjnym do wszystkich urządzeń i serwerów infrastruktury. Ten rodzaj oceny zwykle zapewnia najbardziej wyczerpujące wyniki, ponieważ testerzy nie muszą spędzać czasu w trybie wykrywania. Mają wszystkie informacje, których potrzebują, aby natychmiast rozpocząć dogłębną ocenę.

53. A. Zwykle, gdy NAC jest wdrażany z IPSec, urządzenia sieciowe (takie jak komputery stacjonarne i laptopy) muszą spełniać zasady bezpieczeństwa firmy, zanim będą mogły połączyć się z bezpieczną siecią wewnętrzną. Jeśli tak, otrzymują certyfikat cyfrowy, który pozwala im komunikować się z innymi systemami w bezpiecznej sieci wewnętrznej. W przeciwnym razie są umieszczane w izolowanej sieci naprawczej, dopóki nie uzyskają zgodności. Omijać NAC, przypinanie certyfikatów, może służyć do przypisywania certyfikatu cyfrowego do systemów testerów bez udowadniania, że są one zgodne przy każdym połączeniu.

54. A. Właściwy organ podpisujący w organizacji klienta jest jedyną osobą upoważnioną do wyrażenia zgody na zakres testu penetracyjnego. To, kim właściwie jest, będzie się różnić w zależności od organizacji. Dlatego musisz zweryfikować, czy osoba podpisująca umowę jest faktycznie odpowiednim organem podpisującym dla organizacji. Nie zakładaj, że dana osoba jest upoważniona na podstawie samego stanowiska.

55. A. W tym przykładzie oceniasz tolerancję klienta na wpływy. Włączając to słownictwo do zakresu, chronisz swoją organizację przed sporami sądowymi, jeśli test penetracyjny rzeczywiście wyłączy krytyczne systemy.

56. A i C. W tym scenariuszu wykorzystałeś oszustwo i socjotechnikę, aby uzyskać dostęp do fizycznej sieci organizacji docelowej.

57. C. Credential brute forcing to proces próbowania jednego hasła po drugim, aż w końcu trafisz na właściwe. Może to być wykonywane na kontach użytkowników lub na innych systemach bezpieczeństwa, takich jak sieć bezprzewodowa WPA2, która używa klucza wstępnego.

58. D. Atak słownikowy jest rodzajem ataku brute-force. Jednak w ataku słownikowym wykorzystuje się listę najczęściej używanych haseł, jedno po drugim, w celu odnalezienia właściwego hasła.

59. A. Tęczowa tabela zawiera wstępnie obliczoną listę wartości skrótów dla popularnych haseł, których można użyć do łamania plików haseł offline.

60. A i B. Przemysłowe systemy sterowania (ICS) oraz nadzorcze sterowanie i akwizycja danych (SCADA) są powszechnie stosowane w sprzęcie automatyki przemysłowej i kontroli środowiska. Zwykle działają na starszych systemach operacyjnych, a ich oprogramowanie/oprogramowanie układowe jest

aktualizowane bardzo rzadko. Może to sprawić, że takie systemy będą bardziej podatne na luki w zabezpieczeniach. Zazwyczaj są one również dość delikatne, dlatego należy zachować ostrożność podczas skanowania ich za pomocą skanera luk w zabezpieczeniach.

61. C. Aby zaimplementować exploita porywającego DLL, tester penetracji musi mieć uprawnienia do odczytu/zapisu w docelowym systemie plików. Korzystanie z niezabezpieczonych uprawnień do plików i folderów może znacznie ułatwić wykonanie tego zadania.

62. Porwanie A i D. DLL i zaplanowane zadania mogą pomóc w utrzymaniu trwałości exploita w systemie Windows. Przejęcie DLL powoduje, że exploit zawarty w złośliwej bibliotece DLL jest ładowany za każdym razem, gdy uruchamiana jest podlinkowana aplikacja. Korzystanie z zaplanowanych zadań zapewnia regularne uruchamianie exploita.

63. B. Najlepszą ochroną administratora systemu przed exploitami jądra jest aktualizowanie swoich systemów operacyjnych najnowszymi łatami od producenta. Baza danych Common Vulnerabilities and Exposures (CVE) zawiera informacje o lukach w znanych jądrach systemów operacyjnych Windows, Mac OS, Linux, UNIX, Android i iOS.

64. C. Tester penetracyjny w tym scenariuszu wykorzystywał zaporę sieciową jako brak modyfikacji przez administratora domyślnych ustawień konta na urządzeniu zapory. Większość urządzeń sieciowych, w tym punkty dostępowe, routery, zapory itd., pochodzi z fabryki ze wstępnie skonfigurowanymi domyślnymi poświadczeniami administracyjnymi. Te domyślne ustawienia konta są dobrze udokumentowane w Internecie. Jeśli administrator zapomni je zmienić, tester może je wykorzystać do uzyskania dostępu administracyjnego do urządzenia.

65. B, C i D. Ulepszenie powłoki, ucieczka z maszyny wirtualnej i ucieczka z kontenera to przykłady exploitów ucieczki w piaskownicy.

66. A i E. Możesz wpisać /bin/bash ~/myexploit lub chmod u+x ~/myexploit, aby skrypt się wykonał.

67. B. Polecenie define –i TOTAL utworzy zmienną TOTAL i wpisze ją jako liczbę całkowitą.

68. C. Dodanie polecenia tail /var/log/firewall 1> lastevents 2> &1 do skryptu Bash spowoduje wysłanie zarówno stdout, jak i stderr do tego samego pliku.

69. D. Responder to zestaw narzędzi, który służy do odpowiadania na zapytania NetBIOS z systemów Windows w sieci. Responder to potężne narzędzie do wykorzystywania odpowiedzi NetBIOS. Może on atakować pojedyncze systemy lub całe sieci lokalne, umożliwiając analizowanie lub odpowiadanie na usługi nazw NetBIOS podszywające się pod system, dla którego jest przeznaczone zapytanie.

70. C i E. Istnieje wiele narzędzi, które pomagają w tym kolekcja OSINT:

■ Censys to narzędzie internetowe, które bada adresy IP w Internecie, a następnie zapewnia testerom penetracji dostęp do tych informacji za pośrednictwem wyszukiwarki.

■ Organizacje odcisków palców z zebranymi archiwami (FOCA) to narzędzie typu open source służące do wyszukiwania metadanych w dokumentach pakietu Office, plikach PDF i innych popularnych formatach plików.

■ Maltego to produkt komercyjny, który pomaga w wizualizacji danych zebranych w ramach działań OSINT.

■ narzędzia nslookup pomagają zidentyfikować adresy IP powiązane z organizacją. Recon-ng to modułowa struktura rozpoznania sieci, która organizuje i zarządza pracą OSINT.

■ Shodan to wyspecjalizowana wyszukiwarka umożliwiająca wykrywanie podatnych na ataki urządzeń Internetu rzeczy (IoT) ze źródeł publicznych.

■ theHarvester przeszukuje wyszukiwarki i inne zasoby, aby znaleźć adresy e-mail, nazwiska pracowników i szczegóły dotyczące infrastruktury organizacji.

■ narzędzia whois zbierają informacje z rejestrów publicznych o własności domeny.

71. D. Opcja -h pozwala użytkownikowi na użycie bazy danych Shodan do zapytania o informacje o hoście.

72. D. Chociaż możesz użyć polecenia search do wyszukania słów kluczowych znalezionych w nazwach modułów, poprawną opcją wyświetlenia wszystkich dostępnych modułów jest show modules.

73. A. Wszystkie opcje to typy plików/rozszerzenia obsługiwane przez FOCA, z wyjątkiem .exe, które są plikami wykonywalnymi.

74. D. Skanowanie TCP SYN jest również znane jako skanowanie półotwarte, ponieważ nigdy nie kończy trójetapowego uzgadniania.

75. B. Opcja flagi -p w nmap określi zakres portów. Z drugiej strony użycie -p- zainicjuje pełne skanowanie portów, skierowane na wszystkie możliwe porty (65 535), które mogą być otwarte.

76. A, C. Dwie poprawne odpowiedzi to sklep z aplikacjami Cydia, gdy masz połączenie z Internetem i możesz użyć aplikacji mobilnej Cydia na urządzeniu iDevice, aby pobrać i zainstalować pakiety, oraz dwa, narzędzie Impactor, gdy po raz pierwszy dokonujesz jailbreaku telefonu lub gdy nie masz dostępu do Internetu. Możesz podłączyć przez USB i przeciągnąć i upuścić pliki IPA i zainstalować bezpośrednio na urządzeniu za pomocą Impactora.

77. D. Przynęta jest poprawną odpowiedzią i jest taktyką stosowaną w celu zwabienia ofiar do zrobienia czegoś dla namacalnej nagrody.

78. A, C. SET pomaga ułatwić różne rodzaje ataków socjotechnicznych. Dwa rodzaje ataków, do których może być wykorzystywany, to ataki socjotechniczne oparte na wiadomościach e-mail i SMS. Skanowanie adresów IP i wykonywanie połączeń telefonicznych przez Wi-Fi nie są funkcjami dostępnymi w SET.

79. D. Prawidłowa odpowiedź to wszystkie powyższe. Wszystkie te opcje pomagają złagodzić fizyczne i elektroniczne metody ataków socjotechnicznych.

80. B. Flaga polecenia --rand-source może być użyta do randomizacji adresu źródłowego. Opcja --S ustawia flagę SYN na pakiecie, a --S i --random-source są niepoprawnymi opcjami dla hping3.