1. D i E. Jeśli sama sieć klienta znajduje się w zakresie, musisz zdefiniować identyfikatory SSID sieci bezprzewodowej klienta jako w zakresie. Ważne jest również zdefiniowanie zakresów adresów IP klienta jako in-scope. Nie możesz kierować reklam do stron trzecich, takich jak sąsiedni najemcy lub dostawcy usług w chmurze, bez ich pisemnej zgody.

2. B. Ważne jest, aby wszyscy testerzy penetracji prowadzili starannie spisane dzienniki działań, które podejmują podczas oceny. Dzienniki te powinny identyfikować, co tester zrobił, kiedy to zrobił, jakich systemów używał, jakie systemy atakował i jakie były wyniki. Należy unikać polegania wyłącznie na wspomnieniach testera lub klienta. Zwykle są wadliwe i niekompletne.

3. A. To jest przykład oceny opartej na celu. Celem jest weryfikacja fizycznego bezpieczeństwa organizacji przy użyciu dowolnych środków. Test poprzedzający połączenie jest zwykle przeprowadzany na organizacji przed połączeniem z inną. Test zgodności jest przeprowadzany w celu zapewnienia, że organizacja zachowuje zgodność z przepisami rządowymi lub politykami korporacyjnymi. Test łańcucha dostaw obejmuje testowanie dostawców organizacji.

4. B. W tym scenariuszu wymagana jest ocena zgodności. Jest to ocena oparta na ryzyku, która zapewnia właściwe przestrzeganie zasad lub przepisów. Najprawdopodobniej firmy obsługujące karty kredytowe dostarczą organizacji listę kontrolną, której penetrator użyje do przeprowadzenia oceny. Ocena oparta na celu określi cel, jaki ma osiągnąć test. Ocena łańcucha dostaw obejmuje testowanie dostawców organizacji. Ocena zespołu czerwonego jest zwykle przeprowadzana przez testerów wewnętrznych, aby upewnić się, że personel IT organizacji (zespół niebieski) jest w stanie odpowiednio bronić sieci.

5. B. Przed połączeniem dwóch organizacji często przeprowadza się testy penetracyjne w celu zidentyfikowania wszelkich luk w zabezpieczeniach, które należy usunąć przed połączeniem ich sieci. Celem oceny opartej na obiektywach jest sprawdzenie, czy informacje mogą pozostać bezpieczne. Test zgodności jest przeprowadzany w celu zapewnienia, że organizacja zachowuje zgodność z przepisami rządowymi lub politykami korporacyjnymi. Test łańcucha dostaw obejmuje testowanie dostawców organizacji.

6. C. W tym przykładzie należy wpisać telnet 10.0.0.1 80 w wierszu poleceń powłoki systemu Linux, aby przechwycić baner docelowego serwera WWW.

7. C i E. W tym przykładzie wiesz, że na urządzeniu działa serwer WWW Apache. Zauważ również, że nazwa urządzenia to „Serwer Untangle”. Przeszukując Internet, możesz dowiedzieć się, że Untangle sprzedaje urządzenia zabezpieczające używane do zarządzania ruchem przychodzącym i wychodzącym z sieci. Dlatego można rozsądnie założyć, że urządzenie jest urządzeniem zabezpieczającym tej firmy.

8. B. Urządzenie w tym przykładzie to najprawdopodobniej stacja robocza z systemem Windows. Świadczy o tym fakt, że w systemie są otwarte domyślne porty udostępniania plików SMB/CIFS.

9. C. Urządzenie w tym przykładzie jest najprawdopodobniej kontrolerem domeny działającym w systemie Windows Server. Świadczy o tym fakt, że w systemie są otwarte domyślne porty serwera DNS, LDAP i Kerberos.

10. C i D. Urządzenie w tym przykładzie jest trochę trudniejsze do analizy. Widać wyraźnie, że działa serwer DNS i serwer WWW. Jednak nie wyświetla się tutaj wystarczająca ilość informacji, aby można było wywnioskować wiele innych. Jedną z możliwości jest to, że jest to router bezprzewodowy, który zawiera serwer DNS tylko do buforowania i wbudowany serwer sieciowy, który służy do konfigurowania urządzenia i zarządzania nim. Jednak do dokonania tego ustalenia potrzeba więcej informacji.

11. 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. W tym przykładzie upoważniony pracownik przytrzymał otwarte drzwi dla testera penetracyjnego.

12. 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.

13. D. Skakanie przez płot ma miejsce, gdy nieupoważniona osoba po prostu przeskakuje lub przecina fizyczną barierę zaprojektowaną do kontroli dostępu. W tym scenariuszu tester przebił fizyczną barierę ogrodzenia, wycinając w niej otwór.

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

15. C i D. Do otwarcia zamka potrzebny jest przynajmniej klucz dynamometryczny i wytrych. Klucz dynamometryczny służy do wywierania nacisku obrotowego na zamek (w kierunku odblokowania). Narzędzie do wytrychów służy do zwalniania każdego z kołków w zamku.

16. C. W tym przykładzie narzędzie nmap zostało użyte do uruchomienia skanowania UDP. Dodano jednak opcję –vv, aby znacznie zwiększyć szczegółowość danych wyjściowych.

17. B. W tym przykładzie narzędzie nmap zostało użyte do prostego wyświetlenia listy dostępnych celów. Odbywa się to poprzez uruchomienie nmapa z opcją –sL. Powoduje to, że nmap wyświetla listę hostów, ale nie skanuje ich.

18. C. W tym przykładzie narzędzie nmap zostało użyte do wykrycia dostępnych celów. Odbywa się to poprzez uruchomienie nmapa z opcją –sn. Powoduje to, że nmap wykrywa hosty, ale nie skanuje żadnego z ich portów.

19. A. W tym przykładzie narzędzie nmap zostało użyte do przeskanowania portu 80 na każdym z 10 hostów wymienionych w zakresie adresów IP. Odbywa się to poprzez uruchomienie nmapa z opcją –p 80.

20. C. W tym przykładzie narzędzie nmap zostało użyte do przeskanowania otwartych portów na hoście wymienionym w poleceniu, a następnie określenia wersji usługi przy użyciu każdego z tych portów. Odbywa się to poprzez uruchomienie nmapa z opcją –sV.

21. A. Wdrożenie uwierzytelniania wieloskładnikowego dla połączeń VPN jest przykładem strategii łagodzenia skutków technologii.

22. B. Wdrażanie regularnych szkoleń uświadamiających w zakresie bezpieczeństwa dla wszystkich pracowników jest przykładem strategii łagodzenia opartej na ludziach.

23. C. Wdrażanie procesów off-boardingu pracowników po odejściu z organizacji jest przykładem strategii łagodzenia opartej na procesach.

24. B. Wymaganie od pracowników IT zdania egzaminu certyfikacyjnego w zakresie bezpieczeństwa sieci jest przykładem strategii łagodzenia skutków opartej na ludziach.

25. A. Wymaganie skomplikowanych haseł i wdrażanie ograniczeń konta to przykłady technologicznych strategii ograniczania ryzyka.

26. C. W tym scenariuszu najlepszym podejściem byłoby przeprowadzenie analizy wpływu z klientem i określenie jego tolerancji na wpływ. Czy informacje, które można uzyskać za pomocą skanera luk w

zabezpieczeniach, są warte potencjalnego ryzyka? W przypadku niektórych organizacji ryzyko może być warte korzyści. Dla innych może nie. Tak czy inaczej, penetrator nie powinien korzystać z narzędzia, dopóki analiza wpływu nie zostanie zakończona, a klient jest świadomy ryzyka.

27. B i C. Najprawdopodobniej klient będzie chciał wiedzieć, jakiego rodzaju raport zamierzasz mu dostarczyć po zakończeniu testu. Będą również chcieli wiedzieć, ile czasu zajmie naprawa ich systemów w wyniku testu.

28. B. Zazwyczaj ograniczenia techniczne związane z testami penetracyjnymi identyfikują systemy, które można przetestować i te, których nie można przetestować. Załóżmy na przykład, że klient używa zautomatyzowanego, zrobotyzowanego sprzętu produkcyjnego do wytwarzania swoich produktów. Ten sprzęt jest bardzo drogi i mogą nie chcieć, abyś uwzględnił go w teście.

29. C. Ponieważ jest to test penetracyjny szarej skrzynki, prawdopodobnie powinieneś zapytać klienta, czy chce, aby test został przeprowadzony na miejscu, czy też chce, abyś przetestował go ze zdalnej lokalizacji. Test na miejscu prawdopodobnie przyniósłby lepsze wyniki, ale byłby również droższy, ponieważ testerzy penetracji ponieśliby koszty podróży. Test off-site kosztowałby mniej, ponieważ nie wymagałby kosztów podróży, ale może dać wyniki niższej jakości, ponieważ testerzy nie są fizycznie na miejscu.

30. B. Test czarnoskrzynkowy ma na celu symulację ataku z zewnątrz. Testerzy penetracji powinni mieć taką samą perspektywę, jaką miałby typowy atakujący z zewnątrz. Dlatego powinny być zlokalizowane w podobny sposób, czyli w dowolnej lokalizacji zewnętrznej.

31. C. Fakt, że nie masz poświadczeń administracyjnych, nie oznacza, że musisz zrezygnować z wyliczania i pobierania odcisków palców, ani nie oznacza, że musisz anulować test. Zamiast tego możesz spróbować stworzyć exploit typu spear phishing, aby nakłonić użytkownika wewnętrznego do ujawnienia swoich danych logowania.

32. C. Ponieważ skanujesz tylko serwery internetowe, prawdopodobnie możesz ograniczyć skanowanie luk w zabezpieczeniach tylko do tych portów i protokołów, które są powszechnie używane przez serwery internetowe. Przeprowadzenie dokładnego skanowania wszystkich portów i protokołów zajęłoby znacznie więcej czasu.

33. A i C. Z punktu widzenia topologii sieci standard PCI-DSS wymaga uruchomienia skanowania luk w zabezpieczeniach zarówno z wewnętrznych, jak i zewnętrznych lokalizacji sieciowych. Wyniki obu skanowań należy porównać w celu zidentyfikowania luk w zabezpieczeniach.

34. A. Opcja nmap –Tn służy do określenia szablonu czasowego, gdzie n jest liczbą z zakresu od 0 do 5. Im wyższa liczba, tym szybsze skanowanie podatności. Im niższa liczba, tym wolniejsze skanowanie.

35. C. Ponieważ linia T1 jest ograniczona do 1,54 Mb/s, należy ograniczyć przepustowość wykorzystywaną przez skanowanie luk w zabezpieczeniach. Jeśli tego nie zrobisz, możesz łatwo wykorzystać całą dostępną przepustowość i nie zostawiać jej na krytyczne operacje biznesowe. Możesz użyć opcji –Tn z poleceniem nmap, aby ograniczyć skanowanie. Ze względu na niską przepustowość połączenia, powinieneś rozważyć użycie opcji –T2 lub nawet opcji –T1 z poleceniem nmap. Opcja –T0 prawdopodobnie ograniczyłaby skanowanie zbyt mocno, przez co ukończenie zajęłoby zbyt dużo czasu.

36. D. Wiele urządzeń bezprzewodowych korzysta z systemu Wi-Fi Protected Setup (WPS), aby ułatwić łączenie się z siecią bezprzewodową. Jednak większość implementacji WPS ma kluczową słabość, ponieważ używa prostego ośmiocyfrowego kodu PIN do uwierzytelniania urządzeń bezprzewodowych.

Ze względu na niewielką długość pin można dość szybko złamać, dzięki czemu tester penetracyjny może łatwo połączyć się z docelową siecią bezprzewodową.

37. C. W przypadku bezprzewodowego exploita bluejacking niezamówione wiadomości są wysyłane przez połączenie Bluetooth do urządzeń bezprzewodowych, takich jak telefon komórkowy.

38. B. W przypadku exploita bezprzewodowego bluesnarfing nieautoryzowany Bluetooth nawiązywane jest połączenie z urządzeniem bezprzewodowym, takim jak telefon komórkowy. To połączenie jest następnie wykorzystywane do kradzieży informacji z tego urządzenia.

39. D. W klonowaniu RFID tester penetracyjny przechwytuje podpis RFID z legalnego urządzenia RFID, a następnie kopiuje go do fałszywego urządzenia. Zwykle robi się to w celu skopiowania identyfikatora dostępu RFID.

40. D. Podczas ataku zagłuszającego tester penetracyjny wysyła sygnał radiowy w zakresie częstotliwości 2,4 GHz i/lub 5 GHz, który jest wystarczająco silny, aby zakłócić prawidłowy sygnał bezprzewodowy. To zakłócenie uniemożliwia użytkownikom korzystanie z sieci bezprzewodowej. W związku z tym ten exploit może zostać sklasyfikowany jako test warunków skrajnych sieci lub atak typu „odmowa usługi".

41. B. Odwołując się do wartości zmiennej, Bash używa następującej składni: {$variable_name}. W tym przykładzie komenda echo otrzymuje polecenie wyświetlenia na ekranie wartości zmiennej o nazwie NazwaSerwera.

42. B. Odwołując się do wartości z tablicy, Bash używa następującej składnii: {$array_name[pozycja]}. W tym przykładzie komenda echo otrzymuje polecenie wyświetlenia na ekranie drugiej wartości tablicy o nazwie PrimeNumArray.

43. A. Odwołując się do wartości z tablicy, PowerShell używa następującej składnii: $array_name[pozycja]. W tym przykładzie komenda echo otrzymuje polecenie wyświetlenia na ekranie drugiej wartości tablicy o nazwie PrimeNumArray.

44. D. Odwołując się do wartości z tablicy, Python używa następującej składni: (nazwa_tablicy[pozycja]). W tym przykładzie komenda print otrzymuje polecenie wydrukowania drugiej wartości tablicy o nazwie PrimeNumArray.

45. C. Odwołując się do wartości z tablicy, Ruby używa następującej składni: nazwa_tablicy[pozycja]. W tym przykładzie komenda puts otrzymuje polecenie użycia drugiej wartości tablicy o nazwie PrimeNumArray.

46. A. Aby wzmocnić system serwera, należy upewnić się, że zainstalowane są tylko usługi i aplikacje niezbędne do jego roli. Do sprawdzenia nasłuchiwania portów sieciowych w systemie można użyć polecenia netstat. To pokaże, które usługi są uruchomione w systemie.

47. B. Aby wzmocnić system serwera, należy upewnić się, że wszystkie konta użytkowników mają przypisane hasło. Jednym ze sposobów, aby to zrobić, jest przejrzenie pliku /etc/shadow i wyszukanie kont, do których nie przypisano hasła.

48. D. Aby wzmocnić system serwera, należy upewnić się, że wszystkie przestarzałe konta użytkowników są wyłączone lub usunięte. W tym scenariuszu klient nie chce usuwać kont, ponieważ użytkownicy tymczasowi lub kontraktowi mogą wrócić w przyszłości. Aby ręcznie zablokować konto, możesz użyć polecenia passwd –l, po którym następuje nazwa użytkownika.

49. C. Jednym ze sposobów wzmocnienia systemu serwera jest rekonfiguracja go tak, aby zapisywał wpisy dziennika na dedykowanym serwerze rejestrowania w innym miejscu sieci. Utrudnia to atakującemu zatarcie śladów po włamaniu, ponieważ pliki dziennika nie są przechowywane lokalnie.

50. A. Protokół FTP nie szyfruje przesyłania danych między systemami. Oznacza to, że informacje uwierzytelniające, a także same dane są ujawniane podczas transmisji przez sieć. Aby temu zaradzić, powinieneś zalecić klientowi przełączenie się na FTPS zamiast na FTP. Protokół FTPS używa protokołu SSL lub TLS do szyfrowania sesji FTP, ponieważ szyfrują dane.

51. C. Umieszczenie testerów na białej liście w systemach zapobiegania włamaniom (IPS), zaporom sieciowym aplikacji internetowych (WAF) i innym urządzeniom zabezpieczającym umożliwi im wykonywanie testów bez blokowania. W przypadku testu białej skrzynki oznacza to, że testerzy nie będą spędzać czasu na oczekiwaniu na odblokowanie, gdy środki bezpieczeństwa wykryją ich wysiłki. Testy czarnoskrzynkowe i czerwone zespoły częściej powodują umieszczenie testerów na czarnej liście lub zablokowanie przez środki bezpieczeństwa. W tym scenariuszu tester penetracyjny powinien poinformować klienta, że testowanie powinno koncentrować się na wykrywaniu potencjalnych problemów związanych z bezpieczeństwem we wszystkich systemach objętych zakresem, a nie tylko na określaniu skuteczności aktywnych zabezpieczeń, takich jak IPS.

52. C. SOAP to standard API, który opiera się na XML i powiązanych schematach. Specyfikacje oparte na XML są regulowane przez dokumenty XML Schema Definition (XSD). Posiadanie dobrego odniesienia do tego, co obsługuje konkretny interfejs API, może być cenne dla testera penetracyjnego. To pytanie dotyczy konkretnie plików XML, więc pliki projektu SOAP byłyby najbardziej korzystne.

53. B i E. Znajomość polityki firmy i jej tolerancja na wpływ to dwa najważniejsze elementy, które należy znać podczas planowania zaangażowania. Pozostałe są ważne, ale ten scenariusz wymaga dwóch najważniejszych. Specjaliści od cyberbezpieczeństwa powszechnie zgadzają się, że zarządzanie podatnościami jest kluczowym elementem każdego programu bezpieczeństwa informacji iz tego powodu wiele organizacji nakazuje skanowanie podatności w polityce korporacyjnej, nawet jeśli nie jest to wymóg prawny. Tolerancja ryzyka i wpływu ocenianej organizacji powinna być wykorzystana do określenia zakresu i zasad zaangażowania w ocenę.

54. A. Polityka firmy, zwana również polityką firmy, to udokumentowany zestaw wytycznych, sformułowanych po analizie wszystkich wewnętrznych i zewnętrznych czynników, które mogą wpływać na cele, operacje i plany firmy. Tworzy go zarząd firmy. Polityka korporacyjna określa reakcję firmy na znane i znane sytuacje i okoliczności. Decyduje także o formułowaniu i realizacji strategii oraz ukierunkowuje i ogranicza plany, decyzje i działania kadry kierowniczej firmy w osiąganiu jej celów. W tym scenariuszu polityka firmy powinna być szczegółowa i konkretna; w związku z tym systemy korporacyjne muszą przechowywać hasła przy użyciu algorytmu mieszającego MD5.

55. A. Budżetowanie jest kluczowym czynnikiem procesu biznesowego testów penetracyjnych. Na wykonanie testu penetracyjnego wymagany jest budżet, który zależy od zakresu testu i zasad zaangażowania. W przypadku wewnętrznych testerów penetracyjnych budżet może obejmować tylko czas przydzielony zespołowi na wykonanie testów. W przypadku testerów zewnętrznych budżet zwykle zaczyna się od szacunkowej liczby godzin w oparciu o złożoność testów, wielkość zespołu i wszelkie powiązane koszty.

56. D. Port 21 jest przeznaczony dla TCP i FTP i jest używany jako port kontrolny. Port 80 jest przeznaczony dla TCP i HTTP i jest używany do przesyłania stron internetowych. Port 443 jest używany dla protokołów TCP, HTTPS, HTTP przez TLS/SSL i jest używany do transmisji szyfrowanej. W tym scenariuszu wszystkie porty wykryte przez tester penetracji mają związek z Internetem. Tak więc

odpowiedzią na to pytanie byłoby to, że poufne informacje mogą zostać ujawnione na serwerach internetowych, ponieważ były to porty wskazane podczas skanowania luk w zabezpieczeniach.

57. B. Skanowanie wykrywające identyfikuje systemy operacyjne działające w sieci, mapuje te systemy na adresy IP i wylicza otwarte porty i usługi w tych systemach. Skany wykrywania zapewniają testerom penetracyjnym zautomatyzowany sposób identyfikowania hostów istniejących w sieci i tworzenia inwentaryzacji zasobów.

58. D. Skanowania z poświadczeniami wymagają dostępu tylko do odczytu do serwerów docelowych. Klient powinien kierować się zasadą najmniejszych uprawnień i ograniczać dostęp testera. Powinieneś rozważyć poproszenie o utworzenie konkretnego konta „audytowego" z podobnym dostępem tylko do odczytu. Dedykowane konto „audytowe" ma tę zaletę, że pojawia się w dziennikach i jest natychmiast rozpoznawane przez wszystkich w IT jako potencjalnie zatwierdzona aktywność.

59. D. Testowanie kodu jest często wykonywane przy użyciu statycznej lub dynamicznej analizy kodu wraz z metodami testowania, takimi jak fuzzing i wstrzykiwanie błędów. Po wprowadzeniu zmian w kodzie i jego wdrożeniu należy go ponownie przetestować, aby upewnić się, że zmiany nie spowodowały żadnych nowych problemów z bezpieczeństwem. Ponieważ w tym scenariuszu tylko sprawdzamy kod, przeprowadzimy statyczną analizę kodu. Statyczna analiza kodu, znana również jako analiza kodu źródłowego, odbywa się poprzez przeglądanie kodu aplikacji. Ponieważ analiza statyczna wykorzystuje kod źródłowy, można ją postrzegać jako rodzaj testowania białoskrzynkowego z pełną widocznością. Dzięki temu testerzy mogą znaleźć problemy, których inne testy mogą nie wykryć.

60. B. Dsquery.exe to narzędzie wiersza polecenia służące do wyszukiwania informacji o różnych obiektach w domenie Active Directory. Narzędzie jest domyślnie dostępne we wszystkich wersjach systemu Windows Server. Polecenie dsquery umożliwia przeszukiwanie katalogu LDAP w celu znalezienia obiektów spełniających określone kryteria. Jako atrybut polecenia dsquery musisz określić typ obiektu AD, którego szukasz. W tym scenariuszu szukasz kont użytkowników, które były nieaktywne w ciągu ostatnich 30 dni, więc użyj dsquery user -inactive < NumWeeks >.

61. C. Instrumentacja zarządzania Windows to infrastruktura dostarczana przez Microsoft do centralnego zarządzania systemami Windows przez połączenie sieciowe.

62. C i D. PowerShell (PS) Remoting umożliwia zdalne uruchamianie poleceń cmdlet PowerShell w innych systemach Windows w środowisku sieciowym. Windows Remote Management (WinRM) to system, który umożliwia administratorom systemu Windows zarządzanie systemami zdalnymi przy użyciu protokołu WS Management.

63. B. Protokół RDP (Remote Desktop Protocol) jest używany w systemach Windows do wyświetlania graficznego pulpitu zdalnego hosta Windows w systemie lokalnym za pośrednictwem połączenia sieciowego. Zapewnia pełną interaktywność typu „wskaż i kliknij". Może być nawet używany do przesyłania dźwięków z systemu zdalnego do systemu lokalnego i udostępniania plików między systemami.

64. C. Apple Remote Desktop (ARD) może być używany do zdalnego zarządzania systemami Macintosh przez połączenie sieciowe przy użyciu graficznego interfejsu użytkownika.

65. A. Połączenia Virtual Network Computing (VNC) mogą być używane do zdalnego zarządzania systemami Windows, Macintosh lub Linux przez połączenie sieciowe przy użyciu graficznego interfejsu użytkownika, o ile niezbędne oprogramowanie jest zainstalowane zarówno w systemie lokalnym, jak i zdalnym.

66. A. W bash shell można otworzyć gniazdo sieciowe, aby przekazywać przez nie dane. Gniazdo TCP można otworzyć za pomocą /dev/tcp//. Bash próbuje otworzyć połączenie TCP z odpowiednim gniazdem. Tak więc w tym przykładzie wykonano skanowanie portu. Oto podział kodu:

/bin/bash -i wywołuje interaktywną powłokę bash.

> &/dev/tcp// potoki z powłoką do testera.

0<&1 2>&1 pobiera standardowe wejście i łączy je ze standardowym wyjściem. Następnie określa, aby zrobić to samo ze standardowym błędem (2>).

67. C. Hydra została zaprojektowana tak, aby zawierała obsługę skrótów NTLM jako hasła. Hashcat to narzędzie do łamania i odzyskiwania haseł. Drozer to platforma oceny bezpieczeństwa Androida. Kismet to bezprzewodowy wykrywacz sieci 802.11 warstwy 2, sniffer i system wykrywania włamań. Hydra, często znana jako thchydra, to narzędzie do ataków słownikowych typu brute-force, zaprojektowane do działania przeciwko różnym protokołom i usługom.

68. A. Framework Exploitation Framework (BeEF) jest przeznaczony do tego typu ataków. BeEF zapewnia zautomatyzowany zestaw narzędzi do wykorzystywania socjotechniki w celu przejęcia przeglądarki internetowej klienta. Tester może następnie wykorzystać różne techniki phishingu i socjotechniki, aby zachęcić pracowników do odwiedzenia witryny.

69. A. Generator niestandardowej listy słów (CeWL) to aplikacja w języku Ruby, która umożliwia testerowi przeszukanie witryny internetowej w oparciu o adres URL i ustawienie głębokości, a następnie wygenerowanie listy słów na podstawie znalezionych plików i stron internetowych. Uruchamianie CeWL na stronach internetowych organizacji docelowej może pomóc w wygenerowaniu niestandardowej listy słów. Tworzenie niestandardowej listy słów może być szczególnie przydatne, jeśli zgromadziłeś dużo informacji o swojej organizacji docelowej.

70. A. W tym scenariuszu podane polecenie PowerShell wykona zdalny skrypt. Za pomocą polecenia PowerShell IEX wywoła wyrażenie. Polecenie cmdlet IEX ocenia lub uruchamia określony ciąg jako polecenie i zwraca wyniki wyrażenia lub polecenia. Polecenie cmdlet PowerShell Invoke-Command uruchamia polecenia na komputerze lokalnym lub zdalnym i zwraca wszystkie dane wyjściowe z poleceń, w tym błędy. Używając jednego polecenia Invoke- , możesz uruchamiać polecenia na wielu komputerach.

71. A. Przykład Today() jest funkcją zdefiniowaną przez użytkownika, w której użytkownik jest w stanie rozszerzyć możliwości programu o wykonywanie operacji, które nie są wbudowane w standardowe funkcje dostarczane przez program.

72. C. Today() wywołuje funkcję i wykonuje instrukcję print.

73. B, C. Przed przystąpieniem do ataku socjotechnicznego najlepiej jest upewnić się, że organizacja poddawana tego typu ocenie zatwierdziła wszelkie szablony stron internetowych, e-maili, SMS-ów itp. przed wykonaniem testu. Zasady zaangażowania (RoE) i Oświadczenie o pracy (SOW) to dwa dokumenty, które mogą dostarczyć wskazówek dotyczących tego, co może, a co nie może być dozwolone podczas ataku socjotechnicznego. Umowa o poziomie usług definiuje jakość, dostępność i obowiązki stron uzgadniających, ale najprawdopodobniej nie będzie zawierała szczegółów dotyczących sposobu przeprowadzenia ataku socjotechnicznego ani listy autoryzowanych celów oceny. Regulamin ulepszania nie jest obowiązującym dokumentem i jest błędną odpowiedzią.

74. D. Jest to częsty przykład vishingu lub phishingu głosowego, w którym atakujący próbuje odgrywać rolę innej osoby, która ma pilną sprawę do omówienia lub wymaga natychmiastowej uwagi celu, aby

zmusić ofiarę do zapewnienia żądanych informacji. Spear phishing i wielorybnictwo to rodzaje ataków przeprowadzanych za pośrednictwem poczty elektronicznej, a przynęta to technika motywacyjna, która ma na celu nakłonienie kogoś do zrobienia czegoś w zamian za nagrodę.

75. B, D. VLAN hopping to wektor ataku używany do uzyskania dostępu do zasobów w innej sieci VLAN. Struktura MITER ATT&CK identyfikuje przeskakiwanie VLAN jako technikę ukrywania opartą na sieci (ID: PRE-T1092). Do realizacji przeskakiwania sieci VLAN stosowane są dwie metody: fałszowanie przełączników i podwójne tagowanie.

76. C. Udziały ADMIN$ i C$ są ukrytymi udziałami administracyjnymi ograniczonymi do uprzywilejowanych użytkowników. Choć brzmi to wiarygodnie, akcja HOME$ nie jest typową akcją.

77. B, D. ', -- i ; to zdecydowanie sposoby na wyzwolenie odpowiedzi na błąd z bazy danych, która nie ma filtrowania aplikacji lub bazy danych.

78. C. Opcja -d służy do określenia głębokości przechodzenia do witryny, a -m służy do określenia minimalnej liczby słów identyfikowanych przez narzędzie.

79. D. Najlepszą odpowiedzią jest ?id=..\..\..\..\C:/Windows/boot.ini, ponieważ może pomóc uciec przed podstawowym filtrem treści z ukośnikiem i potencjalnie pokazać zawartość plik boot.ini.

80. A, D, E, F. Clickjacking, Reflected HTML injection, XSS oparty na DOM i przejmowanie sesji to przykłady ataków po stronie klienta. Wstrzykiwanie poleceń i przechodzenie przez katalogi dotyczą luk w zabezpieczeniach po stronie serwera.