1. B. Testy czarnoskrzynkowe są czasami nazywane testami wiedzy zerowej, ponieważ odtwarzają to, co napotkałby typowy atakujący z zewnątrz. Testerzy nie mają dostępu ani informacji. Test białej skrzynki jest wykonywany przy pełnej znajomości sieci bazowej. Test szarej skrzynki może dostarczyć testerom penetracyjnym pewnych informacji o środowisku bez pełnego dostępu. Oceny oparte na celach mają zwykle na celu ocenę ogólnego bezpieczeństwa organizacji.

2. C. Test szarej skrzynki może dostarczyć testerom penetracyjnym pewnych informacji o środowisku bez podawania pełnego dostępu, danych uwierzytelniających lub szczegółów konfiguracji. Oceny oparte na zgodności mają na celu sprawdzenie zgodności z określonymi przepisami. W teście czarnoskrzynkowym testerzy nie mają dostępu ani informacji o środowisku docelowym. Test białej skrzynki jest wykonywany przy pełnej znajomości sieci bazowej.

3. B. W teście czarnoskrzynkowym testerzy nie mają dostępu ani informacji na temat celu. Test białej skrzynki jest wykonywany przy pełnej znajomości sieci bazowej. Test szarej skrzynki może dostarczyć testerom penetracyjnym pewnych informacji o środowisku bez pełnego dostępu. Oceny oparte na celach mają zwykle na celu ocenę ogólnego bezpieczeństwa organizacji.

4. D. Test białej skrzynki jest przeprowadzany z pełną wiedzą o podstawowej technologii, konfiguracji i ustawieniach sieci organizacji docelowej. Test szarej skrzynki może dostarczyć testerom penetracyjnym pewnych informacji o środowisku bez pełnego dostępu. W teście czarnoskrzynkowym testerzy nie mają dostępu ani informacji o środowisku docelowym. Oceny oparte na celach lub obiektywnych są zwykle zaprojektowane do oceny ogólnego bezpieczeństwa organizacji.

5. A. Test szarej skrzynki to połączenie testów czarnej i białej skrzynki. Test szarej skrzynki zwykle dostarcza testerom penetracyjnym ograniczonych informacji o celu, ale nie zapewnia pełnego dostępu, danych uwierzytelniających ani informacji o konfiguracji. Test szarej skrzynki może pomóc skoncentrować czas i wysiłek testerów penetracji, zapewniając jednocześnie dokładniejszy obraz tego, z czym faktycznie może się spotkać osoba atakująca. W teście czarnoskrzynkowym testerzy nie mają dostępu ani informacji o środowisku docelowym. Oceny oparte na celach lub obiektywnych są zwykle zaprojektowane do oceny ogólnego bezpieczeństwa organizacji. Test białej skrzynki jest wykonywany z pełną znajomością podstawowej sieci.

6. A. Censys to narzędzie internetowe, które bada podany adres IP. Przedstawia wszelkie informacje, jakie może wykryć na temat hosta, któremu przypisano ten adres IP, takie jak używana wersja protokołu SSL/TLS, używany zestaw szyfrów i łańcuch certyfikatów. Zwróć uwagę, że niektóre organizacje umieszczają swoje adresy IP na czarnej liście, co poważnie ogranicza ilość informacji, które Censys może znaleźć na ich temat.

7. D. Organizacje odcisków palców z zebranymi archiwami (FOCA) to narzędzie, którego można używać do zbierania metadanych z dokumentów organizacji, takich jak pliki Word, PowerPoint, OpenOffice i Adobe Reader. FOCA przeszukuje popularne wyszukiwarki, takie jak Google i Bing, w poszukiwaniu tych plików i wyodrębnia wszelkie metadane, które mogą zawierać.

8. B. Shodan to specjalistyczne narzędzie, które tester penetracyjny może wykorzystać do przeszukiwania publicznych źródeł dowodów na istnienie urządzenia Internetu rzeczy (IoT), które organizacja docelowa mogła wdrożyć w swojej sieci. Może to być przydatne, ponieważ urządzenia IoT często wykorzystują słabsze mechanizmy bezpieczeństwa, które może wykorzystać tester penetracji.

9. D. Maltego to narzędzie, którego penetratorzy często używają do organizowania informacji zebranych ze źródeł OSINT. Jedną z jego kluczowych zalet jest możliwość graficznego wyświetlania wykrytych informacji i wizualnego łączenia ich ze sobą.

10. A. Narzędzie nmap jest szeroko stosowanym skanerem. Możesz go użyć do skanowania pojedynczego hosta, takiego jak serwer WWW wspomniany w tym scenariuszu, a nawet całej sieci. Aby odnieść sukces jako tester penetracji, powinieneś znać różne sposoby wykorzystania nmapa do odkrywania informacji.

11. D. Przesłuchanie polega na przesłuchaniu pracownika organizacji docelowej, wykorzystując strach jako motywację do zbierania informacji. Przesłuchanie nie jest techniką zwykle używaną przez testerów penetracyjnych.

12. A. Podszywanie się to technika socjotechniczna, którą penetrator może wykorzystać do uzyskania fizycznego dostępu do obiektu celu. W tym scenariuszu recepcjonistka zezwoliła testerowi na dostęp do obiektu organizacji, ponieważ tester wydaje się pochodzić od zaufanego dostawcy.

13. A i E. Podszywanie się to technika socjotechniki, którą może wykorzystać tester penetracyjny w celu uzyskania fizycznego dostępu do obiektu celu. W tym scenariuszu recepcjonistka zezwoliła testerowi na dostęp do obiektu organizacji, ponieważ tester wydaje się pochodzić od zaufanego dostawcy. Tester wykorzystał również techniki pozyskiwania informacji do zbierania poufnych informacji od pracowników.

14. A i C. Podszywanie się to technika socjotechniki, którą penetrator może wykorzystać do uzyskania fizycznego dostępu do obiektu celu. W tym scenariuszu recepcjonistka zezwoliła testerowi na dostęp do obiektu organizacji, ponieważ tester wydaje się pochodzić od zaufanego dostawcy. Tester wykorzystał również techniki „shoppingu na ramieniu", aby zebrać poufne informacje od pracowników.

15. C i E. Podszywanie się to technika socjotechniki, którą może wykorzystać tester penetracyjny w celu zdobycia zaufania pracowników organizacji docelowej. W tym scenariuszu pracownicy ufali testerowi, ponieważ e-maile wyglądały na pochodzące od innego pracownika. Tester wykorzystał to zaufanie, aby uzyskać poufne informacje od tych pracowników. Czasami nazywa się to złamaniem biznesowej poczty e-mail.

16. C. Polecenie nmap 192.168.1.1 -sT powoduje, że narzędzie nmap przeprowadza skanowanie połączenia TCP określonego systemu docelowego.

17. D. Polecenie nmap 192.168.1.1 -sU powoduje, że narzędzie nmap przeprowadza skanowanie portów UDP określonego systemu docelowego.

18. A. Polecenie nmap 192.168.1.0/24 -sL powoduje, że narzędzie nmap skanuje określony zakres adresów IP w poszukiwaniu hostów. Po prostu wyświetla listę celów do skanowania.

19. A. Polecenie nmap 192.168.1.1 -sA powoduje, że narzędzie nmap przeprowadza skanowanie TCP ACK określonego systemu docelowego.

20. C. Polecenie nmap 192.168.1.0/24 --exclude 192.168.1.250 powoduje, że narzędzie nmap skanuje każdy system w podsieci od .1 do .254, ale pomija hosta o adresie IP 192.168.1.250.

21. A. Między innymi termin świadomość sytuacyjna odnosi się do stanu wspólnego zrozumienia między wszystkimi członkami zespołu testującego penetrację, aby zapewnić, że każdy członek zespołu jest świadomy tego, co robią inni.

22. A. Termin świadomość sytuacyjna, między innymi, odnosi się do stanu wspólnego zrozumienia między wszystkimi członkami zespołu testów penetracyjnych w celu zapewnienia koordynacji działań testowych w odpowiednim czasie.

23. B. Termin deeskalacja odnosi się do procesu komunikacji między klientem a testerem w celu zmniejszenia intensywności exploitów wykorzystywanych podczas testu penetracyjnego z powodu niekorzystnego wpływu, jaki mogą one mieć na sieć.

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. C. Między innymi, termin świadomość sytuacyjna odnosi się do stanu wspólnego zrozumienia między wszystkimi członkami zespołu testów penetracyjnych w celu zapewnienia, że działania testowe są planowane i koordynowane tak, aby miały miejsce we właściwym czasie.

26. D. To jest przykład pełzania zakresu. Pełzanie zakresu to dodanie dodatkowych parametrów i/lub celów do zakresu oceny. Jest to częste zjawisko i należy je zaplanować w początkowym ustalaniu zakresu. Na przykład Ty i klient możecie uzgodnić ceny i korekty harmonogramu, które można wprowadzić, jeśli zakres testu będzie wymagał rozszerzenia.

27. A. Wiele narzędzi do testów penetracyjnych może być objętych ograniczeniami eksportowymi. Stany Zjednoczone zabraniają eksportu niektórych typów oprogramowania i sprzętu, w tym narzędzi do szyfrowania. Jeśli podróżujesz za granicę ze swoim zestawem narzędzi do testowania penetracji, możesz zostać aresztowany, jeśli posiadasz zakazane oprogramowanie lub sprzęt.

28. C. Wiele narzędzi do testów penetracyjnych może być objętych ograniczeniami eksportowymi. Stany Zjednoczone zabraniają eksportu niektórych typów oprogramowania i sprzętu, w tym narzędzi do szyfrowania. Jeśli przeniesiesz te narzędzia za granicę przez Internet, możesz zostać aresztowany.

29. D. Prawa i przepisy mające zastosowanie do testów penetracyjnych a testy penetracyjne różnią się w zależności od stanu w Stanach Zjednoczonych. Oznacza to, że musisz zrozumieć, jakie przepisy mają zastosowanie do wykonywanej pracy. W tym scenariuszu musisz sprawdzić wszystkie prawa federalne, stanowe i lokalne, które mają zastosowanie do oceny, którą planujesz przeprowadzić. Zaleca się skorzystanie z usług prawnika, aby uniknąć kłopotów.

30. A. Język opisu usług internetowych (WSDL) jest oparty na języku XML, język definicji interfejsu używany do opisu funkcjonalności oferowanej przez usługę SOAP.

31. A. Zanim Aircrack-ng będzie mógł zostać użyty do złamania szyfrowania w sieci bezprzewodowej, musisz najpierw uruchomić narzędzie airodump-ng na określonym kanale używanym przez transmitujący punkt dostępowy w celu zebrania uzgadniania uwierzytelnienia.

32. B. Zanim Aircrack-ng będzie mógł zostać użyty do złamania szyfrowania w sieci bezprzewodowej, musisz najpierw uruchomić narzędzie airodump-ng na określonym kanale używanym przez transmitujący punkt dostępowy w celu zebrania uzgadniania uwierzytelnienia. Następnie musisz usunąć uwierzytelnienie klienta bezprzewodowego, uruchamiając narzędzie aireplayng.

33. B. Zanim będziesz mógł przechwytywać pakiety w sieci przewodowej, twój interfejs sieciowy musi być skonfigurowany do pracy w trybie promiscuous. W przeciwnym razie odrzuci wszystkie odebrane ramki, które nie są adresowane konkretnie do jego adresu.

34. D. Problem polega na tym, że sieć używa przełącznika zamiast koncentratora. Przełącznik uczy się adresów MAC każdego interfejsu sieciowego podłączonego do każdego portu przełącznika. Przesyła ramki tylko do określonego portu, do którego podłączony jest docelowy interfejs sieciowy. Z tego powodu Twój laptop nigdy nie widzi ramek przesyłanych do innego hosta w sieci.

35. D. Problem polega na tym, że sieć używa przełącznika zamiast koncentratora. Przełącznik uczy się adresów MAC każdego interfejsu sieciowego podłączonego do każdego portu przełącznika. Przesyła ramki tylko do określonego portu, do którego podłączony jest docelowy interfejs sieciowy. Z tego powodu Twój laptop nigdy nie widzi ramek przesyłanych do innych hostów w sieci. Chociaż teoretycznie możesz zamienić przełącznik sieciowy na koncentrator, twój klient prawdopodobnie nie pozwoli ci na to. Najlepszą opcją byłoby podłączenie laptopa do portu lustrzanego na przełączniku. Port lustrzany zawiera kopie ramek przesyłanych do wszystkich pozostałych portów przełącznika. Dzięki temu Twój laptop może zobaczyć ramki zaadresowane do innych hostów. Zanim jednak to zrobisz, musisz upewnić się, że jest to dozwolone zgodnie z zasadami zaangażowania w test.

36. A. NBTSTAT identyfikuje serwery NetBIOS o identyfikatorze . Na podstawie tych wyników wiesz, że DEV-1 jest najprawdopodobniej serwerem Windows (lub serwerem Linux z usługą Samba).

37. B. NBTSTAT identyfikuje stacje robocze NetBIOS za pomocą identyfikatora. Na podstawie tych wyników wiesz, że PROD-9 jest najprawdopodobniej stacją roboczą z systemem Windows (lub stacją roboczą z systemem Linux z uruchomioną usługą Samba).

38. A i E. Protokół LLMNR jest luźno oparty na formacie pakietu DNS i umożliwia hostom IPv4 i IPv6 wykonywanie rozpoznawania nazw dla innych hostów w tej samej sieci lokalnej bez serwera DNS. Jest obsługiwany zarówno przez hosty Windows, jak i Linux.

39. B i C. Protokół LLMNR ma wiele luk w zabezpieczeniach, które można wykorzystać w teście penetracyjnym. Na przykład brakuje kontroli bezpieczeństwa, takich jak uwierzytelnianie. Z tego powodu złośliwy host w sieci może reklamować się jako dowolny host, którego chce.

40. A i C. Protokół Server Message Block (SMB) jest używany do udostępniania plików i drukarek między hostami w sieci.

41. A. Mimikatz można wykorzystać do złamania zabezpieczeń systemów uwierzytelniania opartych na protokole Kerberos, w tym generowania „złotych” i „srebrnych” biletów Kerberos.

42. A i C. Zarówno narzędzia Nikto, jak i W3AF są powszechnie używane do skanowania celów w poszukiwaniu luk.

43. D i E. Zarówno narzędzia Medusa, jak i Hydra mogą być używane do przeprowadzania ataków haseł typu bruteforce.

44. B i D. Zarówno narzędzia Patator, jak i Aircrack-ng mogą być używane do przeprowadzania ataków na hasła typu brute-force. Patator może być używany do łamania zabezpieczeń różnych usług sieciowych, takich jak serwery FTP, SNMP i SSH. Aircrack-ng jest używany do sieci bezprzewodowych typu brute-force.

45. C i D. Zarówno narzędzia Empire, jak i PowerSploit są oparte na środowisku Windows PowerShell. Zasadniczo są one zbiorem skryptów PowerShell, których można używać do przeprowadzania różnych exploitów.

46. B. Prowadzenie szkoleń uświadamiających z pracownikami w zakresie bezpieczeństwa jest przykładem strategii łagodzenia opartej na ludziach.

47. D. Spośród przedstawionych tutaj opcji najlepszym zaleceniem naprawienia udostępnionych poświadczeń administratora lokalnego byłoby po prostu losowanie tych poświadczeń. W przeciwnym razie złamanie hasła administratora lokalnego na jednym komputerze spowoduje ujawnienie wszystkich pozostałych komputerów w organizacji.

48. B. Spośród przedstawionych tutaj opcji najlepszym zaleceniem naprawienia udostępnionych poświadczeń administratora lokalnego byłoby wdrożenie rozwiązania hasła administratora lokalnego (LAPS) firmy Microsoft. To rozwiązanie okresowo losuje hasła lokalnych administratorów i zapisuje te wpisy w Active Directory.

49. B i C. Ustawienia zasad grupy „Hasło musi spełniać wymagania dotyczące złożoności" oraz „Minimalna długość hasła" mogą być użyte do wymuszenia stopnia złożoności hasła. Domyślnie zasada „Hasło musi spełniać wymagania dotyczące złożoności" wymaga, aby hasła miały co najmniej sześć znaków i zawierały znaki z trzech z następujących czterech kategorii: wielkie litery, małe litery, cyfry i znaki specjalne. Minimalna długość hasła określa najmniejszą liczbę znaków, które hasło może zawierać.

50. A. Ustawienie zasad grupy „Wymuszaj historię haseł" określa liczbę unikalnych nowych haseł, których użytkownik musi użyć, zanim będzie można ponownie użyć starego hasła. Skonfigurowanie tej zasady pomaga zwiększyć bezpieczeństwo, uniemożliwiając użytkownikom ponowne używanie starych haseł.

51. A. Specjaliści ds. cyberbezpieczeństwa wykorzystują dobrze znany model triady CIA do opisywania celów bezpieczeństwa informacji. Litera C w CIA oznacza poufność, która ma na celu zapobieganie nieautoryzowanemu dostępowi do informacji lub systemów.

52. B. Specjaliści ds. cyberbezpieczeństwa wykorzystują dobrze znany model triady CIA do opisywania celów bezpieczeństwa informacji. Litera I w CIA oznacza integralność, która ma na celu zapobieganie nieautoryzowanej modyfikacji informacji lub systemów.

53. C. Specjaliści ds. cyberbezpieczeństwa wykorzystują dobrze znany model triady CIA do opisywania celów bezpieczeństwa informacji. Litera A w CIA oznacza dostępność, co zapewnia, że informacje pozostają dostępne dla autoryzowanego dostępu.

54. A. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiadających im celów triady DAD. Pierwsze D w DAD oznacza ujawnienie, które odnosi się do uzyskania nieuprawnionego dostępu do informacji lub systemów.

55. B. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiednich celów triady DAD. Litera A w DAD oznacza zmianę, która odnosi się do dokonywania nieautoryzowanych zmian w informacjach lub systemach.

56. C. Telewizor z dostępem do Internetu jest przykładem nietradycyjnego systemu. Urządzenia te są uważane za kruche, ponieważ trudno nimi zarządzać w tradycyjnym sensie. i prawdopodobnie są one rzadko aktualizowane przez dostawcę. Mogły one również nie zostać poddane obszernym testom bezpieczeństwa przez dostawcę.

57. B. Urządzenia produkcyjne sterowane komputerowo są przykładami systemu nietradycyjnego. Urządzenia te są uważane za delikatne, ponieważ są trudne w zarządzaniu w tradycyjnym sensie i prawdopodobnie są rzadko aktualizowane przez dostawcę. Mogły one również nie zostać poddane obszernym testom bezpieczeństwa przez dostawcę.

58. A i B. Do wykonania transferu strefy można użyć komendy dig axfr @serwer_nazw domena_docelowa lub komenda host -t serwer_nazw_domena_docelowa. Jeśli to zadziała, możesz zebrać dość szczegółową listę wszystkich hostów infrastruktury sieciowej w sieci docelowej. W idealnym przypadku organizacja docelowa wyłączyła nieuwierzytelnione transfery stref na swoim serwerze DNS. W takim przypadku jedno z poprzednich poleceń zwróci jakiś rodzaj komunikatu o błędzie „Transfer nie powiódł się".

59. A. Narzędzie hping jest narzędziem powszechnie używanym przez testerów penetracyjnych do tworzenia pakietów. Pozwala na stworzenie prawie każdego rodzaju pakietu i wysłanie go do wyznaczonego hosta w sieci docelowej. Analiza reakcji hosta może dostarczyć cennych informacji do następnej fazy testu penetracyjnego.

60. A i C. Z listą adresów e-mail użytkowników z targetu organizacji, możesz przeprowadzić dowolną liczbę exploitów phishingowych. Możesz również użyć adresów e-mail do wyliczenia nazw kont użytkowników wewnętrznych. W wielu (jeśli nie większości) organizacjach nazwa użytkownika poczty e-mail jest prawie zawsze taka sama jak nazwa konta użytkownika.

61. C. To jest przykład ataku na domyślne poświadczenia. Większość urządzeń sieciowych, w tym punkty dostępowe, routery, zapory itd., pochodzi z fabryki ze wstępnie skonfigurowanymi domyślnymi poświadczeniami administracyjnymi. Te wartości domyślne są dobrze udokumentowane w Internecie. Jeśli administrator zapomni je zmienić, tester może je wykorzystać do uzyskania dostępu administracyjnego do urządzenia.

62. A. To urządzenie jest podatne na wykorzystanie słabych danych uwierzytelniających, ponieważ nazwa użytkownika i hasło administratora są łatwe do odgadnięcia.

63. D. To jest przykład exploita Kerberos. Otrzymanie biletu nadania biletu (TGT) umożliwia użytkownikowi uzyskanie dodatkowych biletów usługi nadania biletu (TGS), które dają dostęp do określonych usług sieciowych. Ponieważ pozwala użytkownikom uzyskać inne bilety TGS, TGT jest czasami określany jako złoty bilet. Ponieważ bilet TGS może być używany tylko w celu uzyskania dostępu do określonej usługi sieciowej, czasami nazywany jest srebrnym biletem.

64. A i B. Zarówno w przypadku wykorzystania zanieczyszczenia parametrów, jak i niezabezpieczonego bezpośredniego odniesienia do obiektu, tester penetracji modyfikuje parametr w żądaniu HTTP, aby uzyskać nieautoryzowany dostęp do informacji. Na przykład po uwierzytelnieniu w aplikacji internetowej tester może zmodyfikować parametr /search?q= w adresie URL, aby oszukać aplikację w celu podania informacji, których konto użytkownika nie powinno być w stanie zobaczyć.

65. D. W exploitie DOM XSS osoba atakująca wykorzystuje słabości przeglądarki internetowej ofiary. Zazwyczaj przestarzałe przeglądarki są najbardziej podatne na tego typu exploity. Jest to uważane za atak XSS po stronie klienta.

66. A i D. Porównując dwie wartości w skrypcie Pythona, aby sprawdzić, czy nie są one równe, możesz użyć operatora relacyjnego <> lub !=.

67. B. Podczas porównywania dwóch wartości w skrypcie Pythona, aby sprawdzić, czy są one równe, używasz operatora relacyjnego ==.

68. C. Podczas porównywania dwóch wartości w skrypcie PowerShell, aby sprawdzić, czy są one równe, używasz operatora relacyjnego -eq.

69. C. Dokonując porównania między dwiema wartościami całkowitymi w skrypcie Bash, aby sprawdzić, czy jedna jest większa od drugiej, używasz operatora relacyjnego -gt.

70. A. Operator relacyjny > może być użyty zarówno w Pythonie, jak i Ruby do sprawdzenia, czy jedna wartość jest liczbowo większa od drugiej.

71. B i C. W tym scenariuszu router można wzmocnić, tworząc zaszyfrowane hasło dostępu uprzywilejowanego. Odbywa się to za pomocą polecenia enable secret na routerze. Ponadto należy wprowadzić procedury sprawdzające odwiedzających, którzy twierdzą, że są przedstawicielami dostawców IT.

72. A. Po teście penetracyjnym ważne jest, abyś cofnął wszystko, co zrobiłeś. Najlepszym sposobem na osiągnięcie tego jest dokładne udokumentowanie wszystkiego, co robisz podczas przeprowadzania testu. W ten sposób będziesz mieć zapis tego, co należy przywrócić i jak powinno wyglądać po zakończeniu czyszczenia.

73. A i C. Po teście penetracyjnym ważne jest, abyś cofnął wszystko, co zrobiłeś. Na przykład, jeśli skonfigurujesz jakiekolwiek sesje powłoki, zwłaszcza powłoki odwrócone, musisz się upewnić, że zostały one usunięte. Ponadto powinieneś udokumentować wszystko, co robisz podczas sprzątania po teście. Zawsze jest możliwe, że przypadkowo zepsujesz coś podczas procesu czyszczenia. Jeśli tak się stanie, posiadanie dokumentacji tego, co zrobiłeś, będzie nieocenione.

74. B. Po teście penetracyjnym ważne jest, abyś cofnął wszystko, co zrobiłeś. Na przykład, jeśli utworzyłeś jakiekolwiek konta użytkowników backdoora, upewnij się, że usuniesz te poświadczenia. Nie należy pozostawiać ich na miejscu, ponieważ mogą one zostać użyte przez prawdziwego atakującego do późniejszego złamania systemu.

75. A. Po teście penetracyjnym ważne jest, abyś cofnął wszystko, co zrobiłeś. Na przykład bardzo ważne jest odinstalowanie wszelkich narzędzi lub narzędzi używanych do przeprowadzania exploitów podczas testu.

76. A. W czasie działania aplikacja przekaże DOM, aby pomóc uporządkować zawartość w przeglądarce. Moduły DOM mogą zawierać kod JavaScript, który może być wykonywany lokalnie w przeglądarce użytkownika.

77. B. Kod PHP deklaruje zmienną $data poprzez odczytanie 8192 bajtów z $uchwytu. Następnie sprawdza rozmiar zmiennej $data. Jeśli długość $data jest równa 0, skrypt albo kończy działanie, albo kontynuuje powtarzanie zawartości $data i kończy pętlę.

78. A, C. Parametry „acct=” i „emp_id=” są czymś w rodzaju martwego daru Insecure Direct Object Reference (IDOR), ponieważ mogą być połączone z informacjami innego użytkownika, które można pobrać bez koniecznego kontrola dostępu za pomocą aplikacji internetowej lub bazy danych. Opcja B była po prostu adresem URL, z którego nic nie można było wywnioskować, a opcja D zapewniała coś, co wyglądało na parametry związane ze stanem i kodem pocztowym, a nic potencjalna wartość w odniesieniu do identyfikatora IDOR.

79. D. Główna nazwa usługi (SPN) jest unikalna i służy do identyfikowania każdego wystąpienia usługi systemu Windows. W systemie Windows Kerberos wymaga, aby nazwa SPN była skojarzona z co najmniej jednym kontem logowania do usługi. Nazwa hosta to nazwa hosta, a nazwa domeny to unikalna nazwa używana do identyfikacji obszaru w Internecie. Identyfikator użytkownika lub UID to unikalna liczba całkowita przypisana do każdego użytkownika w systemie Unixlike. Żadna z tych opcji nie ma żadnego związku z usługą Windows.

80. A. Po uruchomieniu usługi będzie podążać ścieżką wykonania do: C:\Program Files (x86)\data\shared files\vulnerable.exe, aby uruchomić plik wykonywalny. Ponieważ ścieżka nie

znajduje się w cudzysłowie w rejestrze, najpierw zostanie załadowana C:\Program Files (x86)\data\shared.exe, ponieważ między katalogiem „pliki współdzielone” jest spacja. Files.exe/files.exe nie będzie działać, ponieważ po nazwie katalogu nie ma przerwy. Opcja Program.exe zadziała; jednak użytkownik nie ma dostępu do zapisu w folderze.