1. Robert przeprowadza test penetracyjny w aplikacji internetowej i odkrywa lukę, która pozwala mu zdalnie wyłączyć serwer sieciowy. Jaki cel testów penetracyjnych osiągnął Robert najbardziej bezpośrednio?

A. Ujawnienie

B. Uczciwość

C. Zmiana

D. Odmowa

2. Robert przeprowadził test penetracyjny w szkolnym systemie oceniania i odkrył lukę, która pozwalała uczniom na zmianę ocen

wykorzystując lukę w postaci wstrzyknięcia SQL. Jaki rodzaj kontroli powinien polecić szkolnemu zespołowi ds. cyberbezpieczeństwa, aby uniemożliwić uczniom angażowanie się w tego typu działania?

A. Poufność

B. Uczciwość

C. Zmiana

D. Dostępność

3. Robert zebrał ogromną ilość wrażliwych informacji z Narodowej Agencji Bezpieczeństwa i udostępnił je mediom. Jaki rodzaj ataku przeprowadził?

A. Ujawnienie

B. Odmowa

C. Zmiana

D. Dostępność

4. Zakładając brak istotnych zmian w środowisku danych posiadaczy kart organizacji, jak często PCI DSS wymaga, aby akceptant akceptujący karty kredytowe przeprowadzał testy penetracyjne?

A. Miesięcznie

B. Półrocznie

C. Rocznie

D. Co dwa lata

5. Która z poniższych opcji NIE jest korzyścią z korzystania z wewnętrznego zespołu ds. testów penetracyjnych?

A. Wiedza kontekstowa

B. Koszt

C. Ekspertyza merytoryczna

D. Niezależność

6. Który z poniższych NIE jest powodem do przeprowadzania okresowych testów penetracyjnych systemów i aplikacji?

A. Zmiany w środowisku

B. Koszt

C. Zmieniające się zagrożenia

D. Nowi członkowie zespołu

7. Robert miał ostatnio kłopoty z klientem za użycie narzędzia ataku podczas testu penetracyjnego, który spowodował awarię systemu. Na jakim etapie procesu testów penetracyjnych Robert i jego klienci powinni uzgodnić narzędzia i techniki, których będzie używał podczas testu?

A. Planowanie i ustalanie zakresu

B. Zbieranie informacji i identyfikacja podatności

C. Atakowanie i wykorzystywanie

D. Wyniki raportowania i komunikacji

8. Jaki termin opisuje dokument stworzony w celu zdefiniowania działań specyficznych dla projektu, rezultatów i terminów w oparciu o istniejącą umowę?

A. Umowa o zachowaniu poufności

B. MSA

C. SOW

D. MOD

9. Na jakim typie języka jest oparty WSDL?

A. HTML

B. XML

C. WSML

D. DIML

10. Który z poniższych rodzajów testów penetracyjnych zapewni testerom pełny wgląd w konfigurację serwera WWW bez konieczności narażania serwera na szwank w celu uzyskania tych informacji?

A. Black box

B. Gray box

C. White box

D. Red box

11. Jaki rodzaj umowy prawnej zazwyczaj obejmuje wrażliwe dane i informacje, z którymi tester penetracyjny może się zetknąć podczas przeprowadzania oceny?

A. Zakaz konkurencji

B. Umowa NDA

C. Umowa o bezpieczeństwie danych

D. DSA

12. Który z poniższych podmiotów atakujących jest najbardziej niebezpieczny na podstawie listy poziomów przeciwników?

A. APT

B. Haktywiści

C. Zagrożenia wewnętrzne

D. Przestępczość zorganizowana

13. Podczas testu penetracyjnego Robert odkrywa, że nie jest w stanie przeskanować serwera, który wcześniej udało mu się przeskanować z tego samego adresu IP. Co się najprawdopodobniej wydarzyło?

A. Jego adres IP został umieszczony na białej liście.

B. Serwer uległ awarii.

C. Sieć nie działa.

D. Jego adres IP był na czarnej liście.

14. Robert uruchamia następujący skan Nmapa:

nmap -sU -sT -p 1-65535 example.com

Jakich informacji NIE otrzyma?

A. Usługi TCP

B. Stan usługi

C. Usługi UDP

D. MOD

15. Jaka technika jest używana w następującym poleceniu:

host -t domena axfr.com dns1.domena.com

A. DNS query

B. Nslookup

C. Dig scan

D. Zone transfer

16. Po uruchomieniu skanowania systemu za pomocą Nmapa Robert odkrywa, że porty TCP 139, 443 i 3389 są otwarte. Jaki system operacyjny najprawdopodobniej odkryje w systemie?

A. Windows

B. Androida

C. Linux

D. iOS

17. Robert uruchamia skanowanie Nmap za pomocą następującego polecenia:

nmap -sT -sV -T2 -p 1-65535 example.com

Po obejrzeniu skanowania przez ponad dwie godziny zdaje sobie sprawę, że musi zoptymalizować skanowanie. Który z poniższych sposobów nie jest przydatnym sposobem na przyspieszenie jego skanowania?

A. Skanuj tylko przez UDP, aby poprawić szybkość.

B. Zmień taktowanie skanowania na 3 lub szybsze.

C. Zmień na skanowanie SYN.

D. Użyj domyślnej listy portów.

18. Robert identyfikuje porty TCP 8080 i 8443 otwarte w systemie zdalnym podczas skanowania portów. Jakie narzędzie jest jego najlepszą opcją do ręcznego sprawdzania poprawności działania na tych portach?

A. SSH

B. SFTP

C. Telnet

D. Przeglądarka internetowa

19. Robert odzyskał obraz PNG podczas wczesnej fazy zbierania danych wywiadowczych testu penetracyjnego i chce go zbadać pod kątem użytecznych metadanych. Jakiego narzędzia mógłby najskuteczniej użyć do tego?

A. Narzędzie Exif

B. Grep

C. PsNarzędzia

D. Nginx

20. Podczas skanowania Nmapa Robert używa flagi -O. Skanowanie identyfikuje hosta w następujący sposób:

Działa: Linux 2.6.X

CPE systemu operacyjnego: cpe:/o:linux:linux_kernel:2.6

Szczegóły systemu operacyjnego: Linux 2.6.9 - 2.6.33

Co może ustalić na podstawie tych informacji?

A. Dystrybucja Linuksa zainstalowana w systemie docelowym

B. Poziom poprawek zainstalowanego jądra Linux

C. Data ostatniej aktualizacji systemu zdalnego

D. System działa z jądrem Linuksa 2.6 między .9 a .33

21. Robert przeprowadza test penetracyjny i atakuje serwer bazy danych. Które z poniższych narzędzi najlepiej pomogłoby mu w wykryciu luk w zabezpieczeniach tego serwera?

A. Nessusa

B. Nikto

C. Sqlmap

D. OpenVAS

22. Robert przeprowadza test penetracyjny z czarną skrzynką przeciwko organizacji i zbiera wyniki skanowania podatności do wykorzystania w swoich testach. Które z poniższych skanów najprawdopodobniej dostarczy mu przydatnych informacji w granicach jego testu?

A. Skanowanie wewnętrzne Stealth

B. Pełne skanowanie wewnętrzne

C. Skanowanie zewnętrzne Stealth

D. Pełne skanowanie zewnętrzne

23. Jakiego narzędzia mogą używać testerzy penetracji białej skrzynki, aby pomóc zidentyfikować systemy obecne w sieci przed przeprowadzeniem skanowania luk w zabezpieczeniach?

A. Inwentaryzacja aktywów

B. Ocena aplikacji internetowej

C. Router

D. DLP

24. Robert konfiguruje skanowanie luk w zabezpieczeniach systemu, który podlega standardowi zgodności PCI DSS. Jaka jest minimalna częstotliwość, z jaką musi przeprowadzać skany?

A. Codziennie

B. Co tydzień

C. Miesięcznie

D. Kwartalne

25. Które z poniższych nie jest przykładem narzędzia do skanowania luk w zabezpieczeniach?

A. QualysGuard

B. Snort

C. Nessusa

D. OpenVAS

26. Która z poniższych technologii, zastosowana w organizacji, jest NAJMNIEJ ingerować w wyniki skanowania podatności uzyskane przez zewnętrznych testerów penetracyjnych?

A. Szyfrowanie

B. Zapora sieciowa

C. Konteneryzacja

D. System zapobiegania włamaniom

27. Robert przegląda raport ze skanowania luk w zabezpieczeniach i odkrywa, że jeden z serwerów w jego sieci ma lukę umożliwiającą ujawnienie wewnętrznego adresu IP. Jaki protokół jest prawdopodobnie używany w tej sieci, który spowodował tę lukę?

A. TLS

B. NAT

C. SSH

D. VPN

28. Która z metryk CVSS zawierałaby informacje o tym, ile razy atakujący musi pomyślnie uwierzytelnić się, aby wykonać atak?

A. AV

B. C

C. Au

D. AC

29. Która z poniższych wartości metryki złożoności dostępu CVSS wskazuje, że określony atak jest najłatwiejszy do wykorzystania?

A. i

B. Średni

C. Niski

D. Ciężki

30. Która z poniższych wartości metryki CVSS poufności, integralności lub dostępności wskazuje na możliwość całkowitego narażenia systemu?

A. N

B. A

C. P

D. C

31. Jaka jest najnowsza dostępna obecnie wersja CVSS?

1.0

B. 2,0

C. 2,5

D. 3.0

32. Która z poniższych metryk nie jest uwzględniona w obliczeniach oceny zdolności do wykorzystania w CVSS?

A. Wektor dostępu

B. Wiek podatności

C. Złożoność dostępu

D. Uwierzytelnianie

33. Robert niedawno zidentyfikował nową lukę w zabezpieczeniach i obliczył jej bazowy wynik CVSSv2 na 6,5. Do jakiej kategorii ryzyka należy ta podatność?

A. Niski

B. Średni

C. Wysoki

D. Krytyczne

34. Robert odkrywa ocenę, którą jego skaner podatności wymienia jako 9,3 na 10 w skali ważności. Zidentyfikowana usługa działa na protokole TCP 445. Jakiego typu luki w zabezpieczeniach Robert najprawdopodobniej użyje w tej usłudze?

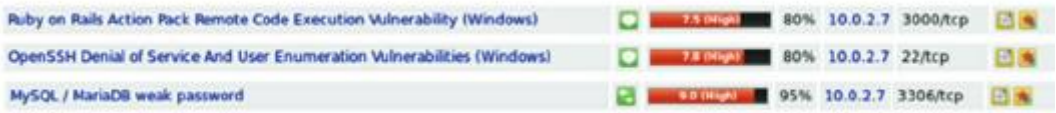
A. Wstrzyknięcie SQL

B. Wykorzystywanie SMB

C. Wykorzystanie CGI

D. Wykorzystanie MIB

Użyj następującego scenariusza dla pytań od 35 do 37. Robert niedawno przeprowadził skanowanie podatności systemu i musi wybrać najlepszą podatność do wykorzystania z poniższego listingu:



35. Które z wpisów z tej listy powinien wybrać Robert, jeśli chce uzyskać dostęp do systemu?

A. Luka Ruby on Rails

B. Luka OpenSSH

C. Luka MySQL

D. Żadne z tych; powinien znaleźć inny cel.

36. Jeśli Robert chce zbudować listę dodatkowych kont użytkowników systemu, która z luk najprawdopodobniej dostarczy te informacje?

A. Luka Ruby on Rails

B. Luka OpenSSH

C. Luka MySQL

D. Luki w zabezpieczeniach OpenSSH i MySQL

37. Jeśli Robert wybierze lukę Ruby on Rails, której z poniższych metod nie można użyć do wyszukania istniejącej luki w Metasploit?

A. CVE

B. BID

C. MSF

D. EDB

38. Robert chce przejść z hosta linuksowego na inne hosty w sieci, ale nie jest w stanie zainstalować dodatkowych narzędzi poza tymi, które można znaleźć na typowym serwerze linuksowym. W jaki sposób może wykorzystać system, na którym się znajduje, aby umożliwić skanowanie podatności tych zdalnych hostów, jeśli są one zabezpieczone zaporą ogniową przeciwko połączeniom przychodzącym i chronione przed bezpośrednim dostępem z jego stacji roboczej do testów penetracyjnych?

A. Tunelowanie SSH

B. Przekierowanie portów NETCAT

C. Włącz IPv6

D. Modyfikuj wtyczki przeglądarki

39. Po uzyskaniu dostępu do systemu Windows Robert używa następującego polecenia:

SchTasks /create /SC Weekly /TN "Antivirus" /TR C:\Users\RKaramagi\av.exe" /ST 09:00

Co osiągnął?

A. Ustawił cotygodniowe skanowanie antywirusowe.

B. Założył pracę o nazwie „co tydzień”.

C. Zaplanował uruchamianie własnego pliku wykonywalnego co tydzień.

D. Nic; to polecenie będzie działać tylko w systemie Linux.

40. Po uzyskaniu dostępu do systemu Linux za pośrednictwem podatnej usługi Robert chce wyświetlić listę wszystkich kont użytkowników w systemie oraz ich katalogów domowych. Która z poniższych lokalizacji zawiera tę listę?

A. /etc/shadow

B. /etc/passwd

C. /var/usr

D. /home

41. Robert chce wdrożyć bezprzewodowy system wykrywania włamań. Które z poniższych narzędzi najlepiej nadaje się do tego celu?

A. WiFite

B. Kismet

C. Aircrack-ng

D. SnortiFi

Użyj poniższego scenariusza do pytań 42, 43 i 44. Robert przeprowadza na miejscu test penetracyjny. Test jest testem szarej skrzynki i może on przebywać na miejscu, ale nie ma dostępu do sieci przewodowych lub bezprzewodowych. Wie, że musi uzyskać dostęp do obu, aby poczynić dalsze postępy.

42. Który z poniższych systemów NAC byłby najłatwiejszy dla Roberta do ominięcia?

A. System oparty na kliencie oprogramowania

B. Serwer proxy DHCP

C. Filtr adresów MAC

D. Żadne z powyższych

43. Jeśli Robert chce założyć fałszywe AP, jakie narzędzie najlepiej odpowiada jego potrzebom?

A. Aircrack-ng

B. Kismet

C. Wireshark

D. WiFite

44. Kiedy Robert uzyska dostęp do sieci, jakiej techniki może użyć do zebrania dodatkowych danych uwierzytelniających?

A. Spoofing ARP, aby stać się man-in-the-middle

B. Podsłuchiwanie sieci za pomocą Wireshark

C. SYN flood

D. Wszystkie powyższe

45. Jaka technika ataku może umożliwić pen-testerowi wgląd w ruch w sieciach VLAN innych niż ich natywna sieć VLAN?

A. Spoofing MAC

B. Podszywanie się pod Dot1q

C. Spoofing ARP

D. Przełącz podszywanie się

46. Jaki rodzaj ataku Bluetooth próbuje wysyłać niechciane wiadomości za pośrednictwem urządzeń Bluetooth?

A. Bluesnarfing

B. Bluesniping

C. Bluejacking

D. Bluesending

47. Robert chce zaatakować system z włączonym WPS. Jakiej techniki ataku może użyć przeciwko niemu?

A. WPSnatch

B. Pixie kurz

C. WPSmash

D. gromadzenie e-Lint

48. Robert chce użyć ataku phishingowego, aby zdobyć referencje należące do wyższego kierownictwa jego celu. Jakiego typu ataku phishingowego powinien użyć?

A. Smishing

B. VIPhishing

C. Whaling

D. Spear phishing

49. Robert chce wejść do centrum danych organizacji o wysokim poziomie bezpieczeństwa. Która z poniższych technik najprawdopodobniej powstrzyma jego próbę tailgatingu?

A. Kamery bezpieczeństwa

B. Mantrapa

C. Czujnik wyjścia

D. Czytnik identyfikatorów RFID

50. Która z poniższych technologii jest najbardziej odporna na ataki polegające na klonowaniu identyfikatorów, jeśli zostanie prawidłowo zaimplementowana?

A. RFID niskiej częstotliwości frequency

B. Magnesy

C. RFID średniej częstotliwości

D. Karty inteligentne

Użyj poniższego scenariusza do pytań 51, 52 i 53. Robert otrzymał zlecenie na wykonanie testu penetracyjnego przeciwko firmie RK, Inc. W ramach testu penetracyjnego poproszono go o przeprowadzenie kampanii phishingowej i wykorzystanie jej wyników kampania mająca na celu uzyskanie dostępu do systemów i sieci RK. Zakres testu penetracyjnego nie obejmuje fizycznego testu penetracyjnego, więc Robert musi pracować całkowicie zdalnie.

51. Robert chce wysłać wiadomość phishingową do pracowników firmy. Chce poznać identyfikatory użytkowników różnych celów w firmie i postanawia do nich zadzwonić, używając sfałszowanego numeru VoIP podobnego do tego, który jest używany w firmie. Kiedy osiąga swoje cele, udaje asystenta

administracyjnego pracującego z jednym z dyrektorów wyższego szczebla RK i prosi swoje cele o informacje o ich koncie e-mail. Co to za socjotechnika?

A. Podszywanie się

B. Przesłuchanie

C. Surfowanie przez ramię

D. Administracja

52. Robert chce wdrożyć złośliwą stronę internetową w ramach swojej próby penetracji, aby móc wykorzystywać przeglądarki należące do pracowników. Jakie ramy najlepiej się do tego nadają?

A. Metasploit

B. BeEF

C. SET

D. OWASP

53. Po próbie zwabienia pracowników RK, Inc., aby dać się nabrać na kampanię phishingową, Robert odkrywa, że nie zdobył żadnych przydatnych danych uwierzytelniających. Postanawia wypróbować keydrop USB. Który z poniższych modułów Socjotechniki powinien wybrać, aby pomóc mu odnieść sukces?

A. Moduł wektorów ataku na strony internetowe

B. Generator zakaźnych mediów

C. Moduł masowych przesyłek pocztowych

D. Moduł ataku Teensy USB HID

54. Które z poniższych podejść, jeśli jest możliwe, jest najskuteczniejszym sposobem na pokonanie ataków iniekcyjnych?

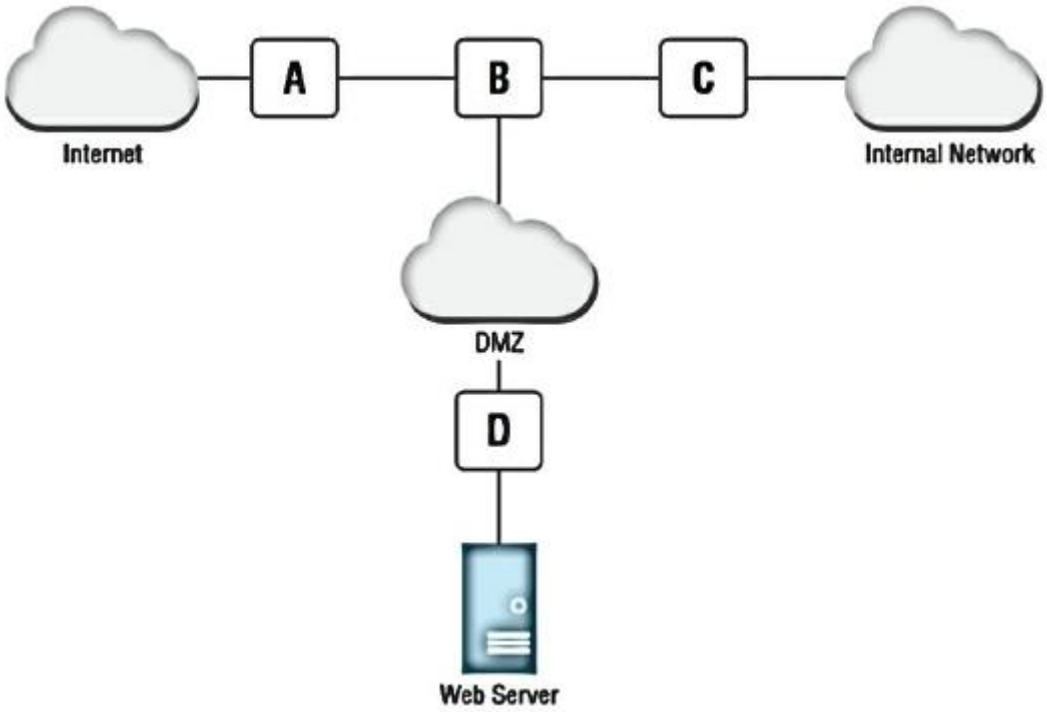
A. Walidacja danych wejściowych w przeglądarce

B. Biała lista danych wejściowych

C. Czarna lista danych wejściowych

D. Wykrywanie podpisu

55. Sprawdź następujący schemat sieci. Jaka jest najodpowiedniejsza lokalizacja zapory aplikacji sieci Web (WAF) w tej sieci?



A. Lokalizacja A

B. Lokalizacja B

C. Lokalizacja C

D. Lokalizacja D

56. Robert sprawdza logi swojego serwera WWW i odkrywa, że użytkownik wysłał dane wejściowe do aplikacji internetowej zawierającej ciąg WAITFOR. Jakiego rodzaju ataku prawdopodobnie próbował dokonać użytkownik?

A. Wstrzyknięcie SQL oparte na czasie

B. Wstrzyknięcie HTML

C. Skrypty między witrynami

D. Wstrzykiwanie SQL oparte na treści

57. Które z poniższych wywołań funkcji jest ściśle związane z atakami wstrzykiwania poleceń Linuksa?

A. system()

B. sudo()

C. mkdir()

D. root()

58. Robert przeprowadza test penetracyjny i próbuje uzyskać dostęp do konta użytkownika. Które z poniższych jest dobrym źródłem uzyskania poświadczeń konta użytkownika?

A. Inżynieria społeczna

B. Domyślne listy kont

C. Zrzuty haseł z zaatakowanych witryn

D. Wszystkie powyższe

59. Jaki rodzaj poświadczeń używanych w Kerberos jest często określany jako „złoty bilet” ze względu na jego potencjał do powszechnego ponownego wykorzystania?

A. Bilet sesyjny

B. Bilet nadający bilet

C. Bilet serwisowy

D. Bilet użytkownika

60. Robert jest testerem penetracji, który chce wziąć udział w ataku polegającym na przejmowaniu sesji. Jakie informacje musi zdobyć Robert, aby jego atak się powiódł?

A. Bilet sesyjny

B. Sesyjny plik cookie

C. Nazwa użytkownika

D. Hasło użytkownika

61. Robert chce zindeksować witrynę swojego celu testów penetracyjnych, a następnie zbudować listę słów, korzystając z danych, które odzyskuje, aby pomóc w łamaniu haseł. Którego z poniższych narzędzi powinien użyć?

A. DirBuster

B. CeWL

C. OLLY

D. Grepomatic

62. Robert chce zaatakować bazowy hiperwizor dla maszyny wirtualnej. Jaki rodzaj ataku ma największe szanse powodzenia?

A. Ucieczka kontenera

B. Naruszyć interfejs administracyjny

C. Hypervisor DoS

D. Ucieczka VM

63. Robert uruchamia ls -l na pliku i widzi następujący listing. Co on wie o chsh?

-rwsr-xr-x 1 root root 40432 27 września 2017 chsh

A. Może służyć do eskalacji uprawnień.

B. Pozwala na odwróconą powłokę.

C. Jest to plik wykonywalny SUID.

D. Żadne z powyższych.

64. Robert chce uzyskać kopię bazy danych SAM systemu Windows z systemu, który naruszył, i na którym działa Metasploit Meterpreter. Jakie dowództwo Mimikatz pozwoli mu to zrobić?

A. meterpreter> mimikatz_command -f samdump::hashes

B. metrpreter> msv

C. meterpreter> mimikatz_command -f samdump::hasła

D. metrpreter> Kerberos

65. Robert chce użyć skanera luk w zabezpieczeniach aplikacji internetowych, aby pomóc w mapowaniu obecności organizacji w sieci i identyfikowaniu istniejących luk w zabezpieczeniach. Które z poniższych narzędzi najlepiej odpowiada jego potrzebom?

A. Paros

B. CUSpider

C. Patator

D. w3af

66. Gdzie znajduje się lista użytkowników Linuksa, którzy mogą korzystać z podwyższonych uprawnień poprzez sudo?

A. /bin/sudo

B. /etc/passwd

C. /etc/sudoers

D. /usr/sudoers

67. Robert chce przeprowadzić atak polegający na porwaniu biblioteki DLL. W którym katalogu system Windows najpierw wyszuka bibliotekę DLL, jeśli nie ma dla niej określonej znanej lokalizacji?

A. Katalog Windows

B. Katalog systemu Windows Windows

C. Katalog, w którym znajduje się aplikacja

D. Aktualny katalog

68. Który z poniższych systemów operacyjnych obsługuje interpretery PowerShell?

A. Linux

B. Mac

C. Windows

D. Wszystkie powyższe

69. Sprawdź następujący wiersz kodu. W jakim języku programowania jest napisany?

print("System zawiera kilka poważnych luk.")

A. Rubin

B. PowerShell

C. Bash

D. Python

70. Sprawdź następujący wiersz kodu. W jakim języku programowania jest napisany? Write-Host „System zawiera kilka poważnych luk w zabezpieczeniach”.

A. Rubin

B. PowerShell

C. Bash

D. Python

71. Które z poniższych stwierdzeń nie opisuje poprawnie języka programowania Ruby?

A. Jest to język programowania ogólnego przeznaczenia.

B. Jest to język tłumaczony.

C. Wykorzystuje skrypty.

D. Jest to język skompilowany.

72. Które z poniższych poleceń pozwoli właścicielowi pliku na wykonanie skryptu Bash?

A. chmod o+e script.sh

B. chmod o+x script.sh

C. chmod u+e script.sh

D. chmod u+x script.sh

73. Która z poniższych zasad wykonywania PowerShell umożliwia wykonanie dowolnego skryptu PowerShell, który piszesz na komputerze lokalnym, ale wymaga, aby skrypty pobrane z Internetu były podpisane przez zaufanego wydawcę?

A. Obejście

B. Nieograniczony

C. Zdalnie podpisany

D. Wszystkie podpisane

74. Który z poniższych wierszy kodu utworzy tablicę w skrypcie PowerShell?

A. $ports = 22, 25, 80, 443

B. ports = (22,25,80,443)

C. ports = [22,25,80,443]

D. $ports= [22,25,80,443]

75. Robert niedawno przeprowadził test penetracyjny dla firmy, która podlega przepisom PCI DSS. Dwa miesiące po teście klient prosi o pismo dokumentujące wyniki testu dla swoich plików zgodności. Jakiego rodzaju raportu żąda klient?

A. Streszczenie wykonawcze

B. Raport z testów penetracyjnych

C. Pisemne świadectwo

D. Poświadczenie ustaleń

76. Robert przegląda wyniki testu penetracyjnego i dowiaduje się, że jego organizacja używa tego samego hasła administratora lokalnego we wszystkich systemach. Które z poniższych narzędzi może pomóc mu rozwiązać ten problem?

A. LAPS

B. Nmap

C. Nessus

D. Metasploit

77. Które z poniższych nie jest normalnym wyzwalaczem komunikacji w teście penetracyjnym?

A. Odkrycie krytycznego odkrycia

B. Zakończenie etapu testowania

C. Dokumentacja nowego testu

D. Identyfikacja wcześniejszego kompromisu

78. Robert przeprowadził skanowanie systemu za pomocą Nmapa i odkrył, że nasłuchuje on na porcie 22, mimo że nie powinien akceptować połączeń SSH. Jakie odkrycie powinien zgłosić?

A. Udostępnione poświadczenia administratora lokalnego

B. Niepotrzebne usługi otwarte open

C. Podatność na wstrzyknięcie SQL

D. Brak uwierzytelniania wieloskładnikowego

79. Wybierz interesariuszy, którzy są zazwyczaj zaangażowani w zaangażowanie typu pentest. (Wybierz dwa.)

A. Użytkownicy

B. Kierownictwo wykonawcze

C. Pentesterzy

D. Zasoby ludzkie

80. Analiza wpływu jest kluczowym aspektem zarządzania wymaganiami i formalnym podejściem do oceny zalet i wad podjęcia działań. Wybierz dwa obszary zainteresowania, które pomogą wesprzeć ćwiczenie pentestu.

A. Budżet organizacyjny

B. Wybór celu

C. Ograniczenia techniczne

D. FISMA