1. Które z poniższych narzędzi NIE jest narzędziem do łamania haseł?

A. OWASP ZAP

B. Cain and Abel

C. Hashcat

D. John the Ripper

2. Który z poniższych skanerów luk w zabezpieczeniach został zaprojektowany specjalnie do testowania zabezpieczeń aplikacji internetowych przed szeroką gamą ataków?

A. OpenVAS

B. Nessusa

C. sqlmap

D. Nikto

3. Które z poniższych narzędzi do debugowania nie obsługuje systemów Windows?

A. GDB

B. OllyDbg

C. WinDbg

D. IDA

4. Jaki jest ostatni etap łańcucha cyberzabójstw?

A. Uzbrojenie

B. Instalacja

C. Działania na rzecz celów

D. Dowodzenie i kontrola

5. Które z poniższych działań zakłada, że organizacja została już zaatakowana?

A. Testy penetracyjne

B. Polowanie na zagrożenia

C. Skanowanie podatności

D. Testowanie oprogramowania

6. Robert tworzy listę zaleceń, które jego organizacja może zastosować, aby rozwiązać problemy zidentyfikowane podczas testu penetracyjnego. W jakiej fazie procesu testowania uczestniczy Robert?

A. Planowanie i ustalanie zakresu

B. Raportowanie i komunikowanie wyników

C. Atakowanie i wykorzystywanie

D. Zbieranie informacji i identyfikacja podatności

7. Dokument umowy na testy penetracyjne, o podpisanie którego Robert prosi swoich klientów, zawiera stwierdzenie, że ocena jest ważna tylko w momencie, w którym ma miejsce. Dlaczego włącza ten język?

A. Jego testowanie może spowodować zmiany.

B. Środowisko prawdopodobnie nie będzie takie samo w przyszłości.

C. Atakujący mogą wykorzystać te same wady do zmiany środowiska.

D. Test nie będzie w pełni wyczerpujący.

8. Jaka strategia testów penetracyjnych jest również znana jako testowanie „z zerową wiedzą”?

A. Testowanie w czarnej skrzynce

B. Testowanie szarej skrzynki

C. Testy w drużynie czerwonej

D. Testowanie w białej skrzynce

9. Organizacja Roberta wykorzystuje technikę, która kojarzy hosty z ich kluczami publicznymi. Jakiej techniki używają?

A. Boks na klucze

B. Przypinanie certyfikatu

C. Blokowanie X.509

D. Prywatność klucza publicznego

10. Robert zakończył ćwiczenie ustalania zakresu swojego testu penetracyjnego i podpisał umowę ze swoim klientem. Czyj podpis powinien być oczekiwany jako kontrasygnat?

A. Funkcjonariusz ds. bezpieczeństwa informacji

B. Sponsor projektu

C. Właściwy organ podpisujący

D. Asystent administracyjny

11. Robert chce się upewnić, że ograniczenia jego testu penetracyjnego prowadzonego przez czerwoną drużynę zostały w pełni wyjaśnione. Które z poniższych są ważnymi zastrzeżeniami dla jego zgody? (Wybierz dwa)

A. Tolerancja na ryzyko

B. Punkt w czasie

C. Kompleksowość

D. Tolerancja na uderzenia

12. W fazie określania zakresu testu penetracyjnego Robert otrzymuje zakres adresów IP systemów, które będzie testował, a także informacje o tym, jakie systemy działają, ale nie otrzymuje pełnego schematu sieci. Jaki rodzaj oceny najprawdopodobniej przeprowadza?

A. Ocena białej skrzynki

B. Ocena kryształowego pudełka

C. Ocena szarej skrzynki

D. Ocena czarna skrzynka

13. Jaki rodzaj oceny najlepiej symuluje wysiłki rzeczywistego napastnika?

A. Ocena czerwonej drużyny ze strategią czarnej skrzynki

B. Ocena oparta na celach ze strategią białej skrzynki

C. Ocena zespołu czerwonego ze strategią kryształowej skrzynki

D. Ocena zgodności ze strategią czarnej skrzynki

14. Robert przeprowadza test penetracyjny dla klienta w Tanzanii. Jakiej karty sieciowej najprawdopodobniej będzie potrzebował, aby sprawdzić informacje o sieciach swojego klienta?

A. RIPE

B. ARIN

C. AFRINIC

D. LACNIC

15. Po przeprowadzeniu przeszukiwania SNMP Robert stwierdza, że nie otrzymał żadnych wyników. Jeśli wie, że nie ma urządzeń zabezpieczających sieć i że są urządzenia, które powinny odpowiadać na zapytania SNMP, jaki problem ma najprawdopodobniej?

A. Ustawiony jest prywatny ciąg SNMP.

B. Nieprawidłowy ciąg społeczności.

C. SNMP działa tylko na porcie 25.

D. Przemiatania SNMP wymagają, aby sieć obsługiwała ruch rozgłoszeniowy.

16. Robert używa następującego polecenia hping do wysyłania ruchu do systemu zdalnego.

hping remotesite.com -S -V -p 80

Jaki rodzaj ruchu zobaczy zdalny system?

A. Ruch HTTP do portu TCP 80

B. TCP SYN do portu TCP 80

C. Ruch HTTPS do portu TCP 80

D. Uzgadnianie trójstronne TCP do portu TCP 80

17. Co oznacza wynik * * * podczas traceroute?

A. Brak trasy do hosta.

B. Zapytali wszyscy gospodarze.

C. Brak odpowiedzi na zapytanie, być może upłynął limit czasu, ale ruch przechodzi.

D. Zapora blokuje odpowiedzi.

18. Robert chce przyjrzeć się reklamowanym trasom do swojego celu. Jakiego rodzaju usługi powinien szukać, aby to zrobić?

A. A BGP looking glass

B. A RIP-off

C. An IGRP relay

D. A BGP tunnel

19. Dlaczego tester penetracyjny miałby szukać wygasłych certyfikatów w ramach ćwiczenia polegającego na zbieraniu informacji i wyliczaniu?

A. Wskazują na niewłaściwe szyfrowanie, umożliwiając łatwe odszyfrowanie ruchu.

B. Wskazują usługi, które mogą nie być odpowiednio aktualizowane lub zarządzane.

C. Atakujący instalują wygasłe certyfikaty, aby umożliwić łatwy dostęp do systemów.

D. Testerzy penetracyjni nie będą szukać wygasłych certyfikatów; wskazują jedynie kwestie proceduralne.

20. Robert uzyskał dostęp do systemu, którego chce użyć do zebrania większej ilości informacji o innych hostach w jego lokalnej podsieci. Chce przeprowadzić skanowanie portów, ale nie może zainstalować w tym celu innych narzędzi. Które z poniższych narzędzi nie nadaje się do skanowania portów?

A. Hping

B. NETCAT

C. Telnet

D. Narzędzie Exif

21. Robert przeprowadza test penetracyjny organizacji i:

przeglądanie kodu źródłowego aplikacji pod kątem luk. Jakie testy kodu prowadzi Robert?

A. Testy mutacji

B. Statyczna analiza kodu

C. Dynamiczna analiza kodu

D. Fuzzing

22. Robert planuje przeprowadzić skanowanie podatności krytycznego systemu biznesowego przy użyciu niebezpiecznych wtyczek. Jakie byłoby najlepsze podejście do wstępnego skanowania?

A. Uruchom skanowanie w systemach produkcyjnych, aby uzyskać jak najbardziej realistyczne wyniki.

B. Uruchom skanowanie w godzinach pracy.

C. Uruchom skanowanie w środowisku testowym.

D. Nie uruchamiaj skanowania, aby uniknąć zakłócenia działalności.

23. Które z poniższych działań nie jest częścią luki?

cykl życia zarządzania?

A. Wykrywanie

B. Remediacja

C. Raportowanie

D. Testowanie

24. Jakie podejście do skanowania podatności obejmuje informacje od agentów działających na docelowych serwerach?

A. Ciągłe monitorowanie

B. Trwające skanowanie

C. Skanowanie na żądanie

D. Alarmowanie

25. Robert stara się określić odpowiednią kategoryzację wpływu dla federalnego systemu informacyjnego, planując kontrolę skanowania podatności dla tego systemu. Po konsultacji z kierownictwem odkrywa, że system zawiera informacje, które w przypadku niewłaściwego ujawnienia miałyby poważny negatywny wpływ na organizację. Jak należy sklasyfikować ten system?

A. Niski wpływ

B. Umiarkowany wpływ

C. Wysoki wpływ

D. Poważny wpływ

26. Robert czyta raporty ze skanów podatności przeprowadzanych przez różne części jego organizacji przy użyciu różnych produktów. Odpowiada za przydzielanie środków zaradczych i ma trudności z ustalaniem priorytetów problemów z różnych źródeł. Jaki komponent SCAP może pomóc Robertowi w tym zadaniu?

A. CVSS

B. CVE

C. CPE

D. XCCDF

27. Robert przeprowadza test penetracyjny i odkrywa krytyczną lukę w aplikacji. Co powinien zrobić dalej?

A. Zgłoś podatność kierownikowi IT klienta

B. Skonsultuj się z SOW

C. Zgłoś usterkę deweloperowi

D. Wykorzystaj lukę

28. Robert wybiera protokół szyfrowania transportu do użycia w nowej publicznej witrynie internetowej, którą tworzy. Który protokół byłby najlepszym wyborem?

A. SSL 2.0

B. SSL 3.0

C. TLS 1.0

D. TLS 1.1

29. Który z poniższych warunków nie spowoduje ostrzeżenia o certyfikacie podczas skanowania luk w zabezpieczeniach serwera WWW?

A. Korzystanie z niezaufanego urzędu certyfikacji

B. Włączenie publicznego klucza szyfrującego

C. Wygaśnięcie certyfikatu

D. Niezgodność nazwy certyfikatu

30. Jaki komponent oprogramowania odpowiada za wymuszanie separacji systemów gościa w infrastrukturze zwirtualizowanej?

A. System operacyjny gościa

B. System operacyjny hosta

C. Kontroler pamięci

D. Hypervisor

31. W jakim typie ataku atakujący chce uzyskać dostęp do zasobów przypisanych do innej maszyny wirtualnej?

A. Ucieczka VM

B. Brutalna siła interfejsu zarządzania

C. Wstrzyknięcie LDAP

D. Wzmocnienie DNS

32. Który z poniższych terminów nie jest zwykle używany do opisania połączenia urządzeń fizycznych z siecią?

A. IoT

B. IDS

C. ICS

D. SCADA

33. Robert odkrywa, że osoba atakująca opublikowała wiadomość atakującą użytkowników odwiedzających forum internetowe, którym zarządza. Który z poniższych typów ataków jest najbardziej prawdopodobny?

A. Wstrzyknięcie SQL

B. Wstrzyknięcie złośliwego oprogramowania

C. Wstrzyknięcie LDAP

D. Cross-site scripting

34. Robert przegląda logi serwera WWW po ataku i znajduje wiele rekordów zawierających średniki i apostrofy w zapytaniach użytkowników końcowych. Jaki rodzaj ataku powinien podejrzewać?

A. Wstrzyknięcie SQL

B. Wstrzyknięcie LDAP

C. Skrypty między witrynami

D. Przepełnienie bufora

35. Robert uruchamia następujące polecenie za pośrednictwem powłoki administracyjnej w systemie Windows, który złamał. Co osiągnął?

$command = 'cmd /c powershell.exe -c Set-WSManQuickConfig-Force;Set-Item

WSMan:\localhost\Service\Auth\Basic-Value $True;Set-Item

WSMan:\localhost\Service\AllowUnencrypted-Value $True;Register-PSSessionConfiguration-Name

Microsoft.PowerShell — życie"

A. Włączył PowerShell dla użytkowników lokalnych.

B. Założył PSRemoting.

C. Wyłączył zdalny dostęp do wiersza poleceń.

D. Założył WSMan.

36. Podczas przygotowań do fazy exploitów testu penetracyjnego Robert odkrywa szereg luk w zabezpieczeniach umożliwiających ujawnienie informacji. Jeśli nie był w stanie zidentyfikować informacji o użytkowniku lub usłudze poza szczegółami dotyczącymi luk w zabezpieczeniach, jaki priorytet powinien nadać ich wykorzystaniu?

A. Wysoki priorytet; wykorzystać wcześnie.

B. Średni priorytet; exploit po próbie wykorzystania innych systemów i usług.

C. Niski priorytet; wykorzystuj tylko wtedy, gdy pozwala na to czas.

D. Nie wykorzystuj; exploity związane z ujawnianiem informacji nie są warte przeprowadzania.

37. Część zakresu prac Roberta w zakresie testów penetracyjnych i zasady

zaangażowanie umożliwia mu fizyczny dostęp do testowanego obiektu. Jeśli nie może znaleźć usługi, którą można wykorzystać zdalnie, która z poniższych metod socjotechniki najprawdopodobniej spowoduje zdalny dostęp?

A. Nurkowanie w śmietniku

B. Phishing

C. Upuszczenie pendrive

D. Podszywanie się pod numer pomocy technicznej

38. Robert chce przechwytywać skróty użytkownika w sieci Windows. Jakie narzędzie mógłby wybrać, aby zebrać je z wiadomości rozgłoszeniowych?

A. Metasploit

B. Responder

C. Impacket

D. Wireshark

39. Robert chce znaleźć exploita frameworka Metasploit, który nie spowoduje awarii usługi zdalnej, której jest celem. Jaki ranking musi osiągnąć lub przewyższyć wybrany przez niego exploit, aby to zapewnić?

A. Doskonały

B. Świetnie

C. Dobrze

D. Normalny

40. Robert chce użyć tęczowych tablic przeciwko przechwyconemu plikowi haseł. Jak tęczowe tablice łamią hasła?

A. Odszyfrowywanie haseł

B. Porównanie skrótów w celu zidentyfikowania znanych wartości

C. Odszyfrowywanie haseł

D. Testowanie haszów metodą brute-force

41. Podczas testu penetracyjnego Robert używa podwójnego tagowania w celu przesłania ruchu do innego systemu. Jakiej techniki on próbuje?

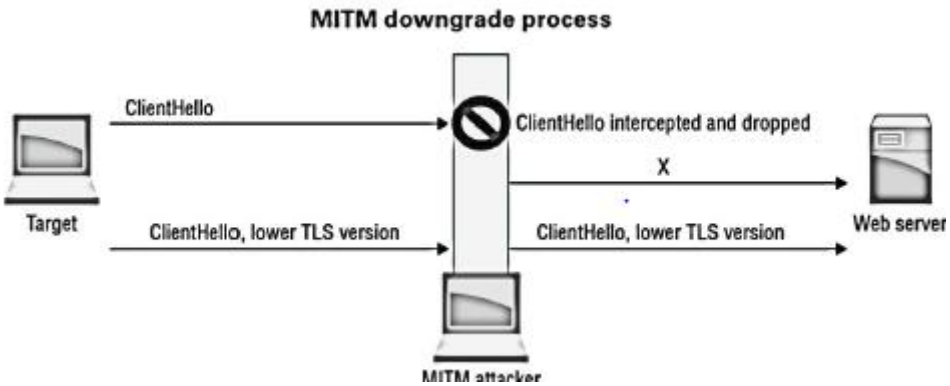
A. Znakowanie RFID

B. Zagnieżdżanie tagów

C. Metatagowanie

D. Przeskakiwanie VLAN

42. Robert umieścił swoją stację roboczą jako mężczyzna pośrodku, jak pokazano na poniższym obrazku. Co musi wysłać w punkcie X, aby upewnić się, że atak downgrade działa poprawnie?



A. SYN, ACK

B. PSH, URG

C. FIN, POTWIERDZENIE

D. SYN, FIN

43. Robert chce użyć arpspoof do przeprowadzenia ataku typu man-in-the-middle między docelowym hostem 10.0.1.5 a serwerem 10.0.1.25 z bramą sieciową 10.0.1.1. Jakie polecenia musi uruchomić, aby to zrobić? (Wybierz dwa.)

A. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.25

B. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.1

C. arpspoof -i eth0 -t 255.255.255.255 -r 10.0.1.25

D. arpspoof -i eth0 -t 10.0.1.25 -r 10.0.1.5

44. Robert chce wylistować politykę haseł domeny dla domeny Windows. Jakiego polecenia net może do tego użyć?

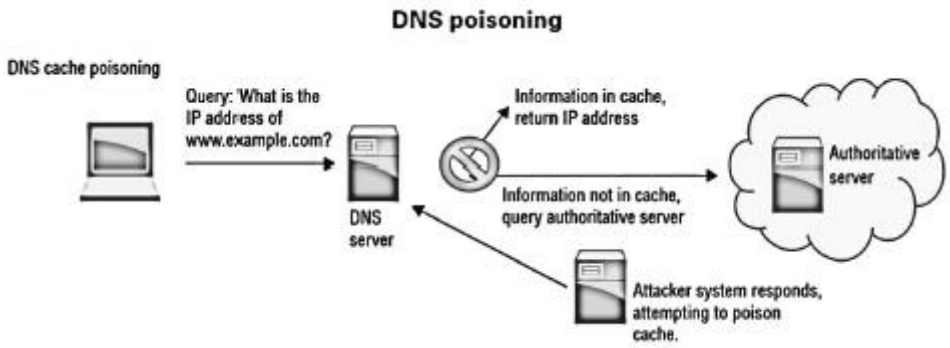
A. net view /domainpolicy

B. net accounts /domain

C. net /viewpolicy

D. net domain /admin

45. Robert próbował przeprowadzić atak zatrucia DNS, jak pokazano tutaj. Po próbie nie widzi żadnego ruchu z systemu docelowego. Co najprawdopodobniej spowodowało niepowodzenie ataku?



A. Informacje DNS były nieprawidłowe.

B. Zastrzyk był zbyt wolny.

C. Pamięć podręczna DNS nie została odświeżona.

D. Klient nie otrzymał zaufanej odpowiedzi.

46. Robert chce sklonować kartę dostępu RFID. Jaki typ karty najłatwiej sklonować za pomocą niedrogich urządzeń do klonowania?

A. Karta o niskiej częstotliwości od 125 do 134,2 KHz

B. Karta średniej częstotliwości 400 do 451 KHzHz

C. Karta wysokiej częstotliwości 13.56 MHz MHz

D. Karta o bardzo wysokiej częstotliwości 865 do 928 MHz MHz

47. Robert wysyła wiadomość phishingową do organizacji docelowej i zawiera wiersz „Tylko pięciu respondentów otrzyma nagrodę pieniężną". Jakiej strategii motywacyjnej socjotechniki używa?

A. Niedobór

B. Dowód społeczny

C. Strach

D. Władza

48. Co dzieje się podczas próby socjotechniki quid pro quo?

A. Cel otrzymuje pieniądze.

B. Cel jest proszony o pieniądze.

C. Cel sprawia, że czuje się zadłużony.

D. Tester penetracyjny sprawia, że czuje się zadłużony.

49. Robert wie, że pracownicy jego firmy docelowej często odwiedzają popularny w okolicy portal dyskusyjny poświęcony piłce nożnej. W ramach testów penetracyjnych z powodzeniem umieszcza w witrynie złośliwe oprogramowanie i przejmuje wiele komputerów należących do pracowników. Jakiego rodzaju ataku użył?

A. Atak PWNie

B. Atak chłodnicy wodnej

C. Atak klonów

D. Atak wodopoju

50. Robert nieumyślnie uruchamia alarm i zostaje wykryty przez ochroniarza podczas testu penetracyjnego na miejscu. Jaka powinna być jego pierwsza odpowiedź?

A. Zadzwoń na policję

B. Próba ucieczki

C. Podaj pretekst

D. Zadzwoń do jego osoby kontaktowej organizacyjnej

51. Upuszczenie klucza USB jest przykładem jakiego rodzaju techniki?

A. Fizyczny honeypot

B. Wyczyn humanitarny

C. Nurkowanie z odwróconym śmietnikiem

D. Atak hybrydowy

52. Robert dzwoni do pracowników firmy, której zlecono mu przeprowadzenie kampanii phishingowej, skupiającej się na osobach w dziale finansowym. W ciągu kilku dni przekonuje pracownika do wysłania przelewu na konto, które założył, po tym, jak powiedział pracownikowi, że poinformował szefa o jego talentach. Jakiej techniki motywacyjnej użył?

A. Pośpiech

B. Wzajemność

C. Władza

D. Strach

53. Robert uważnie zwraca uwagę na pracownika, który wpisuje swój kod dostępu do obszaru o wysokim poziomie bezpieczeństwa docelowej organizacji i zapisuje obserwowany przez niego kod. Jaki rodzaj ataku przeprowadził?

A. Atak na astronomię Setec

B. Nadzór kodu

C. Surfowanie na ramieniu

D. Przechwytywanie klawiatury

54. Który z poniższych ataków jest przykładem wykorzystywania warunków rasowych?

A. XSRF

B. XSS

C. TOCTTOU

D. SQLi

55. Robert jest programistą, który tworzy kod do publicznej sprzedaży. Chciałby zapewnić swoich użytkowników, że kod, który otrzymują, faktycznie pochodzi od niego. Jakiej techniki może użyć, aby najlepiej zapewnić to zapewnienie?

A. Podpisywanie kodu

B. Potwierdzenie kodu

C. Szyfrowanie kodu

D. Zaciemnianie kodu

56. Które z poniższych narzędzi jest narzędziem do statycznej analizy kodu?

A. YASCA

B. Peach

C. Immunity

D. WinDBG

57. Robert przeprowadza test penetracyjny aplikacji internetowej i chciałby manipulować danymi wejściowymi wysyłanymi do aplikacji, zanim opuści ona jego przeglądarkę. Które z poniższych narzędzi pomogłoby mu w tym zadaniu?

A. AFL

B. ZAP

C. GDB

D. DOM

58. Jaka kontrola jest najczęściej używana do zabezpieczania dostępu do interfejsów API?

A. Klucze API

B. Hasła

C. Wyzwanie-odpowiedź

D. Uwierzytelnianie biometryczne

59. Które z poniższych narzędzi do debugowania jest zgodne z systemami Linux?

A. WinDBG

B. GDB

C. OllyDbg

D. SonarQube

60. Podczas testu penetracyjnego Robert odkrywa w dzienniku serwera WWW, że testerzy próbowali uzyskać dostęp do następującego adresu URL:

http://www.mycompany.com/sortusers.php?file=C:\uploads\attack.exe

Jaki rodzaj ataku najprawdopodobniej podjęli?

A. Odbity XSS

B. Trwałe XSS

C. Włączenie plików lokalnych

D. Zdalne włączenie pliku file

61. Co jest wymagane, aby Robert przeprowadził atak zimnego rozruchu na system?

A. Zdalny dostęp

B. Temperatury poniżej 32 stopni Celsjusza

C. Dostęp fizyczny

D. System musiał być wyłączony przez ponad 30 minut.

62. Podczas gdy Robert przeprowadza test penetracyjny, uzyskuje dostęp do serwera Windows Deployment Services dla swojej organizacji docelowej. Jakich krytycznych informacji może się spodziewać po znalezionych tam nienadzorowanych plikach instalacyjnych?

A. Hasła administratora domeny

B. Hasła użytkowników lokalnych

C. Hasła administratora lokalnego

D. Hasła użytkowników domeny

63. Na jaką podatność powinien namierzyć Robert, jeśli odkryje usługę z następującym wierszem w wywołaniu systemowym?

Zmienna ścieżki = "C:\Program Files\CommonPliki\przykładaplikacja\przykład.exe"

A. Przejęcie DLL

B. Usługa zapisywalna

C. Zmodyfikowany zwykły tekst

D. Nienotowana ścieżka usługi

64. Robert chce użyć ataku brute-force na usługę SSH świadczoną przez jeden z jego celów. Które z poniższych narzędzi nie jest przeznaczone do usług typu bruteforce?

A. Patator

B. Hydra

C. Meduza

D. Minotaur

65. Po zhakowaniu zdalnego hosta Robert używa ssh, aby połączyć się z portem 4444 ze swojej stacji roboczej do testów penetracyjnych. Jaki rodzaj zdalnej powłoki skonfigurował?

A. reverse shell

B. root shell

C. bind shell

D. blind shell

66. Robert chce złamać skróty z pliku haseł, który odzyskał podczas testu penetracyjnego. Która z poniższych metod będzie zazwyczaj najszybsza, zakładając, że zna metodę mieszania i ma odpowiednie pliki i narzędzia, aby wykorzystać każde narzędzie?

A. John the Ripper

B. Rainbow Crack

C. Hashcat

D. CeWL

67. Przeanalizuj następujący segment kodu:

```
Do{
$test='mike' + $i
$cracked = Test-Password $test
$i++
}
While($cracked -eq 0 )
```

W jakim języku jest napisany ten kod?

A. Rubin

B. PowerShell

C. Python

D. Bash

68. Przeanalizuj następujący segment kodu:

```
if [ $weekday==1 ]
then
/usr/local/bin/nmap 192.168.1.1
elif [ $weekday==3 ]
then
/usr/local/bin/nmap 192.168.1.2
else
/usr/local/bin/nmap 192.168.1.0/24
fi
```

W jakim języku jest napisany ten kod?

A. Rubin

B. PowerShell

C. Python

D. Bash

69. Przeanalizuj następujący segment kodu:

```
for hst in range(0,256):
```

```
ip= net + str(hst)

print(ip, ': ', socket.gethostbyaddr(ip), '\n'))
```

W jakim języku jest napisany ten kod?

A. Rubin

B. PowerShell

C. Python

D. Bash

70. Jakiego polecenia uniksowego można użyć do nasłuchiwania danych wejściowych na porcie sieciowym?

A. grep

B. sed

C. awk

D. nc

71. Który z poniższych języków programowania nie oferuje wbudowanej solidnej możliwości obsługi błędów?

A. PowerShell

B. Python

C. Rubin

D. Bash

72. Jaka wartość zostałaby użyta do zakodowania znaku ampersand w ciągu adresu URL?

A. %24

B. %25

C. %26

D. %27

73. Jaki operator porównania testuje, aby sprawdzić, czy jedna liczba jest większa lub równa innej liczbie w Bash?

A. -gt

B. -ge

C. >

D. >=

74. Która z poniższych nie jest powszechną kategorią działań remediacyjnych?

Ludzie

B. Proces

C. Testowanie

D. Technologia

75. Która z poniższych technik nie jest odpowiednim działaniem naprawczym w przypadku luki w zabezpieczeniach SQL injection?

A. Zapora sieciowa

B. Odkażanie wejściowe

C. Walidacja danych wejściowych

D. Zapytania parametryczne

76. Kiedy powinny odbywać się działania wzmacniające system?

A. Kiedy system jest początkowo zbudowany

B. Kiedy system jest początkowo budowany i okresowo w trakcie jego życia

C. Kiedy system jest początkowo zbudowany i kiedy jest wycofany z eksploatacji

D. Kiedy system jest budowany po raz pierwszy, okresowo w trakcie jego eksploatacji i gdy jest wycofywany z eksploatacji

77. Technologia uwierzytelniania biometrycznego pasuje do tego, co wieloczynnikowe

kategoria uwierzytelniania?

A. Coś, co wiesz

B. Coś, czym jesteś

C. Gdzieś jesteś

D. Coś, co masz

78. Biała i czarna lista to mechanizmy kontroli dostępu, które można zaimplementować we wszystkich poniższych przypadkach z wyjątkiem _____.

A. Zapory sieciowe

B. Zapory aplikacji

C. Identyfikatory SSID

D. Filtry spamu

E. Oprogramowanie do skanowania wirusów

79. Umowa ramowa o świadczenie usług (MSA) jest umową nadrzędną, która może zawierać zestawienie prac (SOW) opisujące konkretne działania związane z pracą w ramach projektu. W której części SOW znajdziesz działania związane z pracą nad projektem?

A. Zakres prac

B. Harmonogram wyników

C. Wymagania specjalne

D. Kryteria akceptacji

80. W którym dokumencie można znaleźć pisemne upoważnienie, które daje zespołowi pentestacyjnemu upoważnienie do kontynuowania zadania?

A. MSA

B. RoE

C. SOW

D. MBA