1. Tester penetracyjny używa typowego konta e-mail pracownika do wysyłania e-maila phishingowego do menedżerów i kadry kierowniczej w organizacji docelowej. Celem jest sprawdzenie, ilu faktycznie zainteresowało się exploitem, i kliknięcie odsyłacza w wiadomości. Jaki rodzaj testu penetracyjnego jest wykonywany w tym scenariuszu?

A. Black box

B. Gray box

C. White box

D. Red box

2. Pracujesz dla firmy zajmującej się testami penetracyjnymi. Klient dzwoni i prosi o wykonanie wyczerpującego testu, który dokładnie przebada jego infrastrukturę pod kątem luk w zabezpieczeniach. Jaki rodzaj testu powinieneś polecić?

A. Gray box

B. White box

C. Black box

D. Blue box

3. Określasz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Będzie to ocena w białej skrzynce. To będzie test wewnętrzny. Żadne strony trzecie nie mogą być zaangażowane. Które z poniższych zasobów można uznać za mieszczące się w zakresie oceny? (Wybierz dwa.)

A. Użytkownicy Active Directory

B. Zasady haseł zdefiniowane w Zasadach Grupy

C. Aplikacje chmurowe Microsoft Office 365

D. Dokumenty Google

E. Serwery internetowe Microsoft Azure

4. Jaki jest najważniejszy krok w procesie planowania i ustalania zakresu testów penetracyjnych?

A. Uzyskanie pisemnego upoważnienia od klienta

B. Pisanie zasad zaangażowania (ROE)

C. Wybór metodologii testowania

D. Definiowanie systemów, aplikacji i dostawców usług objętych i poza zakresem

5. Który z poniższych dokumentów jest formalnym dokumentem, który dokładnie określa, co zostanie zrobione podczas testu penetracyjnego?

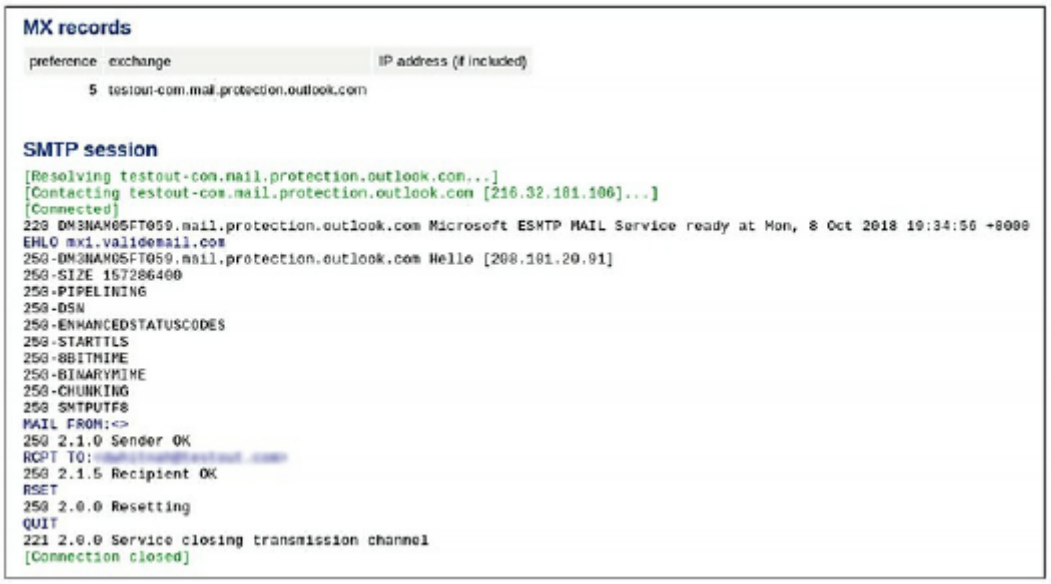
A. Ramowa umowa serwisowa (MSA)

B. Umowa o zachowaniu poufności (NDA)

C. Zestawienie pracy (SOW)

D. Zamówienie zakupu (PO)

6. Podczas fazy wykrywania testu penetracyjnego wykorzystującego czarną skrzynkę zidentyfikowałeś adres e-mail, który, jak podejrzewasz, należy do kierownictwa w organizacji docelowej. Korzystasz ze strony centralops.net, aby przeanalizować ten adres e-mail. Wyniki są pokazane tutaj:



MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:[redacted]
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

Czego możesz się nauczyć z wyników?

A. Serwer poczty e-mail organizacji ma adres IP 208.101.20.106.

B. Serwer poczty e-mail organizacji znajduje się za urządzeniem filtrującym pocztę e-mail.

C. Serwer poczty e-mail organizacji działa w systemie Windows i ma otwarte porty 80 i 443 w zaporze.

D. Serwer poczty e-mail organizacji odpowiada na polecenia HELO.

7. Podczas testu penetracji białej skrzynki używasz narzędzia nmap do skanowania całej podsieci w poszukiwaniu hostów. Po zakończeniu skanowania musisz wyliczyć znalezione systemy. Jakie informacje musisz zidentyfikować dla każdego wykrytego urządzenia? (Wybierz dwa.)

A. Zainstalowane usługi

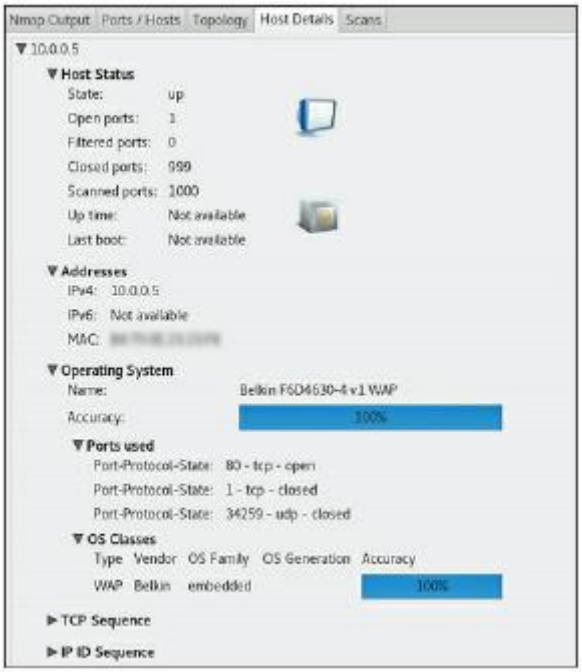
B. Wersja nmapa użyta do wykonania skanowania

C. Liczba unikalnych użytkowników w podsieci

D. Wersja zainstalowanego systemu operacyjnego

E. Klasa kabla Ethernet użytego do stworzenia sieci fizycznej

8. Podczas fazy wykrywania testu penetracyjnego szarej skrzynki używasz narzędzia Zenmap do wyliczenia i odcisku palca urządzeń w jednej z podsieci organizacji docelowej. Szczególnie jedno urządzenie przykuło Twoją uwagę. Wynik jest pokazany tutaj:



Czego możesz dowiedzieć się o urządzeniu z tych informacji?

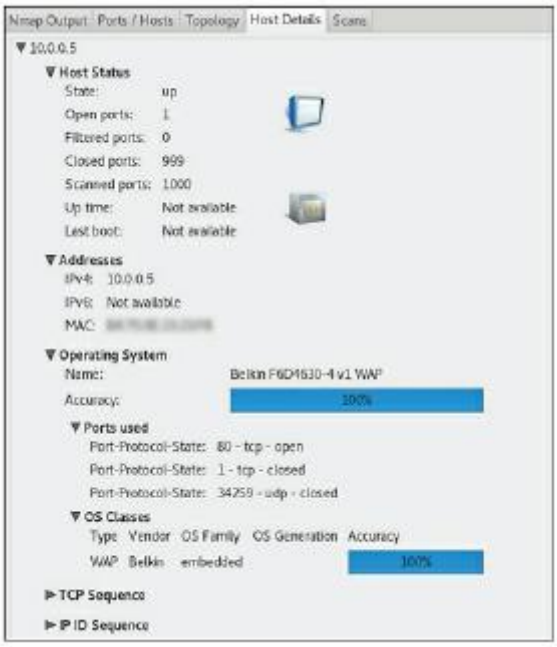
A. Jest to serwer Windows.

B. Jest to maszyna wirtualna.

C. To jest router.

D. Jest to punkt dostępu do sieci bezprzewodowej.

9. Podczas fazy wykrywania testu penetracyjnego szarej skrzynki używasz narzędzia Zenmap do wyliczenia i odcisku palca urządzeń w jednej z podsieci organizacji docelowej. Szczególnie jedno urządzenie przykuło Twoją uwagę. Wynik jest pokazany tutaj:



Czego możesz dowiedzieć się o urządzeniu, korzystając z tych informacji?

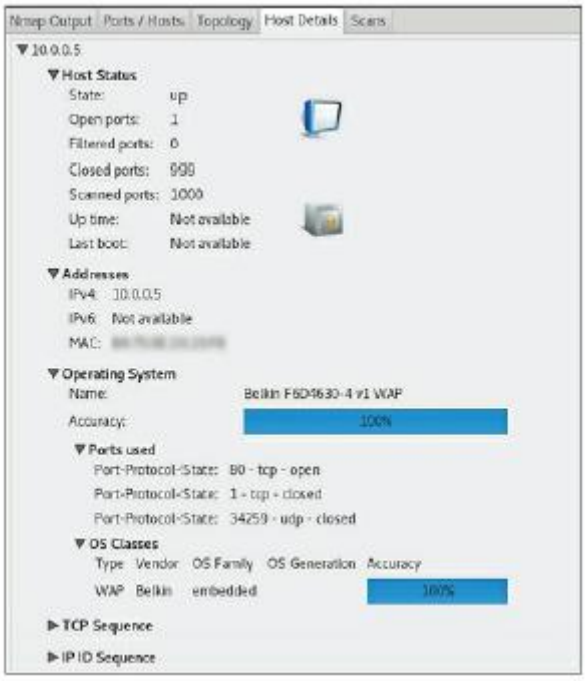
A. Urządzenie jest w trybie konserwacji.

B. Działa usługa HTTP.

C. Został dołączony do domeny Windows.

D. Jest zarządzany przez kontroler bezprzewodowy.

10. Podczas fazy wykrywania testu penetracyjnego szarej skrzynki używasz narzędzia Zenmap do wyliczenia i odcisku palca urządzeń w jednej z podsieci organizacji docelowej. Szczególnie jedno urządzenie przykuło Twoją uwagę. Wynik jest pokazany tutaj:



Czego możesz dowiedzieć się o urządzeniu, korzystając z tych informacji?

A. Domyślne hasło administratora urządzenia

B. Liczba podłączonych klientów bezprzewodowych

C. Adres IP kontrolera urządzenia

D. Marka i model kontrolera urządzenia

11. Jaki czynnik motywacyjny skłania ludzi do działania, ponieważ martwią się konsekwencjami niedziałania?

A. Dowód społeczny

B. Strach

C. Niedobór

D. Władza

12. Tester penetracyjny wchodzi do fizycznego obiektu docelowej organizacji, przechodząc za pracownikiem i chwytając drzwi zabezpieczone uwierzytelnianiem, zanim całkowicie się zamkną. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

13. Penetracja wchodzi do fizycznej placówki docelowej organizacji, nawiązując rozmowę z pracownikiem na parkingu i przechodząc z nią przez drzwi, które wykorzystują czytnik kart zbliżeniowych do kontroli dostępu. Pracownik otwiera drzwi za pomocą swojego identyfikatora i przytrzymuje je przed testerem penetracyjnym. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

14. Penetracja czeka na parkingu docelowej organizacji, aż zobaczy dużą grupę pracowników wracających z lunchu. Wchodzi cicho z tyłu grupy. Pierwsza osoba w grupie używa swojej odznaki, aby otworzyć zabezpieczone drzwi. Tester penetracyjny jest w stanie przejść przez drzwi z resztą grupy. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

15. Gdy tester penetracyjny zbliża się do głównego wejścia do obiektu fizycznego docelowej organizacji, zauważa, że do kontroli dostępu używany jest kołowrót. Ostrożnie przechodzi przez bramkę, zamiast przez nią przechodzić. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Skakanie przez płot

16. Która opcja powoduje, że nmap skanuje przy użyciu małych, pofragmentowanych pakietów w celu oszukania zapory filtrującej pakiety?

A. -f

B. -Pn

C. -n

D. -sC

17. Która opcja powoduje, że nmap wysyła skany ze sfałszowanego adresu IP?

A. -f

B. -D

C. -n

D. -sF

18. Która opcja powoduje, że nmap skanuje określoną liczbę losowych hostów?

A. -iL

B. -sS

C. -sR

D. -iR

19. Która opcja powoduje, że nmap skanuje hosta w poszukiwaniu 100 najczęściej używanych portów IP, takich jak 20, 21, 23, 25, 53, 80 itd.?

A. -pB. -sV

C. -F

D. -p 100

20. Która opcja nmap powoduje, że narzędzie przekazuje połączenia przez serwer proxy?

A. – pełnomocnicy

B. -S

C -D

D. -g

21. Generujesz pisemny raport ustaleń po teście penetracyjnym. W oparciu o samą liczbę luk, które wykryłeś w teście, uważasz, że klient powinien przejść kolejny test penetracyjny w ciągu najbliższych trzech miesięcy, aby sprawdzić, czy problemy zostały naprawione. Gdzie zamieścić tę rekomendację w raporcie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

22. Właśnie skończyłeś pisać raport wyników dla klienta po teście penetracyjnym. Jak długo Twoja organizacja musi przechowywać dokument po zakończeniu testu?

A. Sześć miesięcy

B. Jeden rok

C. Pięć lat

D. Zależy od umowy z klientem

23. Właśnie skończyłeś pisać raport wyników dla klienta po teście penetracyjnym. Który z poniższych sposobów jest odpowiednim sposobem przechowywania pisemnego raportu z ustaleń Twojego klienta?

A. Wydrukuj kopię i trzymaj ją w teczce na biurku.

B. Zapisz go na dysku flash, który jest przechowywany w uchwycie na długopis na biurku.

C. Nagraj go na dysk optyczny wielokrotnego zapisu i przechowuj w szufladzie biurka.

D. Zapisz go w zaszyfrowanym pliku na serwerze plików.

24. Właśnie skończyłeś pisać raport wyników dla klienta po teście penetracyjnym. Który z poniższych sposobów jest odpowiednim sposobem przechowywania pisemnego raportu z ustaleń Twojego klienta?

A. Wydrukuj kopię i przechowuj ją w zamkniętej szafce na dokumenty, która została przykręcona do podłogi.

B. Zapisz go na swoim koncie dysku Google.

C. Zapisz go w pliku na swoim laptopie.

D. Nagraj go na dysk optyczny wielokrotnego zapisu i przechowuj w pojemniku na płyty CD na biurku.

25. Właśnie skończyłeś pisać raport wyników dla klienta po teście penetracyjnym. Który z poniższych sposobów jest odpowiednim sposobem przechowywania pisemnego raportu z ustaleń Twojego klienta?

A. Nagraj raport na dysk optyczny i przechowuj go w zamkniętym sejfie przykręconym do biurka.

B. Zapisz plik na zaszyfrowanym dysku flash.

C. Skopiuj plik do telefonu.

D. Zapisz raport do pliku na pulpicie stacji roboczej.

26. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Które z poniższych testów należy uwzględnić w ocenie?

A. Zainstaluj i zaktualizuj oprogramowanie antywirusowe we wszystkich systemach.

B. W środowisku używaj wyłącznie routerów Cisco z certyfikatem bezpieczeństwa.

C. Zamknij wszystkie porty z wyjątkiem 139 i 445 w zaporze, która chroni środowisko danych posiadacza karty (CDE).

D. Wyłącz monitorowanie dostępu do danych posiadacza karty.

27. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Które z poniższych testów należy uwzględnić w ocenie?

A. Musi istnieć polityka haseł.

B. Zamknij wszystkie porty z wyjątkiem 80 i 443 w zaporze, która chroni środowisko danych posiadacza karty (CDE).

C. Wszystkie hosty w sieci muszą mieć domyślną bramę.

D. Wszystkie hosty w sieci muszą mieć unikalny adres hosta.

28. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Które z poniższych testów należy uwzględnić w ocenie? (Wybierz dwa.)

A. Monitoruj wszelki dostęp do danych posiadacza karty.

B. Upewnij się, że WPA2 jest używane do zabezpieczania wszystkich sieci bezprzewodowych.

C. Upewnij się, że TKIP służy do zabezpieczania wszystkich sieci bezprzewodowych.

D. Ograniczenie dostępu do danych posiadacza karty na zasadzie niezbędnej wiedzy.

29. Które prawo reguluje, w jaki sposób instytucje finansowe traktują dane osobowe klientów?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

30. Które prawo wymaga, aby organizacje związane z opieką zdrowotną spełniały określone standardy bezpieczeństwa?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

31. Wykonujesz skanowanie podatności podczas testu penetracyjnego szarej skrzynki. Skaner manipuluje trójetapowym uzgadnianiem protokołu TCP w celu wyliczenia hostów sieciowych. Jaki rodzaj skanowania wykonujesz?

A.Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

32. Wykonujesz skanowanie podatności podczas testu penetracyjnego szarej skrzynki. Skaner manipuluje trójetapowym uzgadnianiem protokołu TCP w celu wyliczenia hostów sieciowych. Najpierw skaner wysyła pakiet SYN do hosta docelowego. Host odpowiada pakietem SYN-ACK do hosta skanującego. Co się potem dzieje?

O. Host skanujący odpowiada hostowi docelowemu pakietem ACK.

B. Host docelowy wysyła do hosta skanującego pakiet ACK.

C. Host skanujący wysyła pakiet ICMP Echo Request do hosta docelowego.

D. Host skanujący odpowiada hostowi docelowemu pakietem RST.

33. Przeprowadzasz test penetracji szarej skrzynki. Przeprowadzasz skanowanie luk w zabezpieczeniach sieci wewnętrznej za pomocą skanowania ukrytego. W sieci docelowej zainstalowane jest urządzenie IDS. Co może się wydarzyć?

A. IDS wykryje skanowanie z ukrycia.

B. Skanowanie stealth pozostanie niewykryte przez IDS.

C. IDS zablokuje ruch z Twojego systemu skanującego.

D. Skanowanie stealth ustanowi pełne połączenia TCP z każdym hostem w sieci docelowej.

34. Jaki typ skanowania podatności daje najdokładniejsze wyniki?

A. Odkrycie

B. Pełny

C. Ukrycie

D. Nieuwierzytelnione

35. Klient wynajął Cię do wykonania testu penetracyjnego PCI-DSS. Jakiego rodzaju skanowanie podatności wykonałbyś podczas tego testu?

A. Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

36. Podczas testu penetracyjnego szarej skrzynki tester postanawia przeprowadzić test warunków skrajnych krytycznego routera sieciowego. Wysyła tysiące żądań ping skierowanych do wszystkich hostów w podsieci. Jednak fałszuje adres źródłowy żądań do adresu IP routera sieciowego. W rezultacie router jest zalewany ruchem odpowiedzi ICMP echo, którego nie zainicjował, co utrudnia mu odpowiadanie na uzasadnione żądania sieciowe. Co to za exploit?

A. Odmowa usługi (DoS)

B. Rozproszona odmowa usługi (DDoS)

C. Powtórz atak

D. Obejście NAC

37. Które z poniższych uniemożliwia nieautoryzowanym lub niesprawnym urządzeniom łączenie się z siecią, nawet jeśli prawidłowo łączą się z siecią przewodową lub bezprzewodową?

A. Kontrola dostępu do sieci (NAC)

B. WPA2-PSK

C. Wirtualne sieci LAN (VLAN)

D. Protokół drzewa opinającego (STP)

38. Podczas testu penetracyjnego szarej skrzynki próbujesz podłączyć laptopa do sieci bezprzewodowej celu. Jednak cel zaimplementował NAC, który blokuje połączenie laptopa z siecią produkcyjną. Co możesz zrobić?

A. Przeprowadź atak brute-force z odszyfrowaniem, aby pokonać szyfrowanie IPSec, które chroni sieć produkcyjną.

B. Sfałszuj swój laptop adresem MAC autoryzowanego urządzenia.

C. Podłącz laptopa do przewodowego gniazda.

D. Stwórz zły bliźniak punkt dostępowy.

39. Jakie typy urządzeń sieciowych są często umieszczane na białej liście w wielu implementacjach NAC? (Wybierz dwa.)

A. Laptopy

B. Komputery stacjonarne

C. Serwery

D. Telefony VOIP

E. Urządzenia SCADA

40. Która metoda jest powszechnie używana do przeskakiwania między sieciami VLAN?

A. Podwójne znakowanie

B. Ataki siłowe

C. Podszywanie się pod adres MAC

D. Zatrucie DNS

41. Które narzędzie do testowania penetracji jest narzędziem do wyszukiwania z wiersza poleceń internetowej bazy danych Exploit-DB znanych exploitów?

A. Znajdź błędy

B. Shodan

C. Censys

D. Splot wyszukiwania

42. Podczas testu penetracyjnego szarej skrzynki tester chce zatruć zapytania dla kontrolera domeny organizacji docelowej w celu przekierowania żądań klientów do laptopa testera i przechwytywania nazw użytkowników i zaszyfrowanych haseł. Jakiego narzędzia można do tego użyć?

A. Searchsploit

B. Empire

C. Impacket

D. Responder

43. Które narzędzie do testowania penetracji składa się ze zbioru klas Pythona używanych do niskopoziomowego dostępu do protokołów sieciowych, takich jak SMB?

A. Searchsploit

B. Empire

C. Impacket

D. Responder

44. Które narzędzie do testów penetracyjnych zapewnia testerom penetracyjnym ogromną liczbę exploitów, które można wykorzystać do włamania się do sieci organizacji docelowej?

A. Framework Metasploit

B. SET

C. hping

D. ncat

45. Podczas czytania wykonywalnego pliku skryptu, w pobliżu początku skryptu widzisz wiersz, który deklaruje zmienną przy użyciu następującej składni:

NazwaSerwera = FS1

Jaki to może być rodzaj skryptu? (Wybierz dwa.)

A. PowerShell

B. Bash

C. Rubin

D. Python

46. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich odkryciach informujesz, że serwer sieciowy Linux w centrum danych ma uruchomiony serwer sieciowy Apache, bazę danych MySQL, usługi DNS, CUPS, DHCP, IMAP i POP3. Co powinieneś polecić klientowi, aby zaradzić tej sytuacji?

A. Odinstaluj wszystkie niepotrzebne usługi z serwera.

B. Zamknij porty w zaporze opartej na hoście serwera związane z niepotrzebnymi usługami.

C. Odinstaluj usługi DNS i DHCP.

D. Odinstaluj usługi związane z pocztą e-mail.

47. Serwer Windows działa jako kontroler domeny Active Directory dla sieci organizacji. Które z poniższych usług nie są wymagane do pełnienia tej roli? (Wybierz dwa.)

A. Zarządzanie zasadami grupy

B. Hyper-V

C. Narzędzia do administrowania rolami

D. Usługi federacyjne Active Directory

48. Które z poniższych są typowymi metodami stosowanymi do wzmacniania kont użytkowników w systemie komputerowym z systemem Windows? (Wybierz dwa.)

A. Użyj zasad grupy, aby skonfigurować blokadę konta.

B. Włącz anonimową translację SID/nazwy.

C. Włącz wbudowane konto użytkownika Gość.

D. Włącz anonimowe wyliczanie kont i udziałów SAM.

E. Usuń lub wyłącz wszystkie nieużywane konta użytkowników.

49. Które z poniższych są typowymi metodami stosowanymi do wzmacniania kont użytkowników w systemie komputerowym z systemem Windows? (Wybierz dwa.)

A. Wymagaj od użytkowników uwierzytelniania przy użyciu internetowych kont użytkowników Microsoft.

B. Użyj zasad grupy, aby wymusić wymagania dotyczące złożoności hasła.

C. Zezwalaj na stosowanie uprawnień „wszyscy” do anonimowych użytkowników.

D. Użyj zasad grupy, aby wymusić wymagania dotyczące starzenia się haseł.

E. Zezwalaj standardowym użytkownikom na instalowanie aktualizacji

50. Która z poniższych metod jest powszechnie stosowana do wzmacniania komunikacji sieciowej w systemach komputerowych z systemem Windows?

A. Włącz NetBIOS przez TCP/IP.

B. Zezwól na anonimowy dostęp do udostępnionych folderów.

C. Przechowuj wartości skrótu LAN Managera.

D. Ustaw poziom uwierzytelniania LAN Manager, aby umożliwić LM i NTLM.

E. Ogranicz dostęp do sieci tylko do uwierzytelnionych użytkowników.

51. Negocjujesz nadchodzący test penetracyjny z nowym klientem. Poprosili o wykonanie testu „częściowej wiedzy” o ich sieci. Jaki rodzaj testu penetracyjnego należy wykonać?

A. Black box

B. Grey box

C. White box

D. Oparte na celach

52. Negocjujesz nadchodzący test penetracyjny z nowym klientem. Poprosili o wykonanie testu „pełnej wiedzy” o ich sieci. Jaki rodzaj testu penetracyjnego należy wykonać?

A. Black box

B. Grey box

C. White box

D. Na podstawie celu

53. Planujesz nadchodzący test penetracyjny białej skrzynki z nowym klientem. Ich sieć wykorzystuje kontrolę dostępu do sieci (NAC) przy użyciu protokołu IPSec. Którą technikę będą musieli zastosować Twoi testerzy penetracji, aby umożliwić im dostęp do bezpiecznej sieci wewnętrznej chronionej przez NAC?

A. Przypinanie certyfikatu

B. Przejmowanie sesji

C. Człowiek pośrodku

D. Cross-site scripting

54. Pracujesz dla firmy zajmującej się testami penetracyjnymi. Sprawdzałeś nadchodzący test penetracyjny z klientem. Współpracowałeś z dyrektorem ds. informatyki, aby określić zakres oceny, taki jak systemy mieszczące się w zakresie i poza nim, stosowana metodologia, dozwolone techniki i harmonogram. Masz gotowy projekt umowy gotowy do podpisania. Kto powinien to podpisać?

A. Właściwy organ podpisujący

B. Kierownik IT

C. CIO

D. Każdy pracownik helpdesku może podpisać umowę.

55. Pracujesz dla firmy zajmującej się testami penetracyjnymi. Sprawdzałeś nadchodzący test penetracyjny z klientem. W dokumencie dotyczącym zakresu dołączasz słowne ostrzeżenie, że metodologia i techniki użyte w tym teście mogą potencjalnie spowodować wyłączenie krytycznych systemów na pewien czas. Prosisz klienta o potwierdzenie, że jest to dopuszczalne. Jaki jest ten przykład?

A. Ocena tolerancji na uderzenia

B. Zastrzeżenie dotyczące kompleksowości

C. Wyłączenie odpowiedzialności w określonym momencie

D. Zasady wypełniania oceny

56. Przeprowadzasz test penetracji czarnej skrzynki. Po uzyskaniu dostępu do sieci wewnętrznej i przeprowadzeniu skanowania luk w zabezpieczeniach zidentyfikowałeś system docelowy i zmapowałeś jego luki do konkretnego exploita. Jednak do wykonania exploita potrzebny jest fizyczny dostęp do

wewnętrznego gniazda sieciowego. Więc wjeżdżasz na ogon do ośrodka, podłączasz laptopa i uruchamiasz exploit. Jakiej techniki użyłeś w tym scenariuszu? (Wybierz dwa.)

A. Oszustwo

B. Modyfikacja exploitów

C. Inżynieria społeczna

D. brutalne forsowanie poświadczeń

E. Opracowanie dowodu koncepcji

57. Która z poniższych technik polega na przesyłaniu jednego hasła po drugim w systemie uwierzytelniania w celu znalezienia właściwego?

A. Rainbow table

B. Teardrop attack

C. Credential brute-forcing

D. SYN attack

58. Która z poniższych technik polega na wysyłaniu kolejno haseł z listy najczęściej używanych haseł w celu odnalezienia właściwego?

A. Rainbow table

B. SYN attack

C. Man-in-the-middle attack

D. Dictionary attack

59. Która z poniższych pozycji jest wstępnie obliczoną listą wartości skrótu dla popularnych haseł, których można użyć do łamania plików haseł offline?

A. Rainbow table

B. Fingerprint

C. Digital signature

D. Private key

60. Które z poniższych są specjalnymi urządzeniami sieciowymi, które są powszechnie używane do sterowania urządzeniami produkcyjnymi i systemami środowiskowymi? (Wybierz dwa.)

A. ICS

B. SCADA

C. Punkt sprzedaży

D. RTOS

E. IoT

61. Który z poniższych problemów może umożliwić testerowi penetracji wykonanie exploita przechwytującego DLL w systemie Windows?

A. Niepowodzenie instalacji najnowszych aktualizacji systemu Windows

B. Używanie nieaktualnych definicji wirusów

C. Korzystanie z niezabezpieczonych uprawnień do plików i folderów

D. Brak konfiguracji ograniczeń konta użytkownika w zasadach grupy

62. Która z poniższych technik może pomóc w zachowaniu trwałości exploita w systemie Windows? (Wybierz dwa.)

A. Korzystanie z zaplanowanych zadań

B. Używanie ataków zimnego rozruchu

C. Implementacja Kerberoastingu

D. Korzystanie z przejmowania bibliotek DLL

E. Szukanie exploitów jądra

63. Jaki jest najlepszy sposób obrony przed exploitami jądra?

A. Zaktualizuj definicje antywirusowe systemu.

B. Zainstaluj najnowsze aktualizacje systemu operacyjnego.

C. Używaj bezpiecznych uprawnień do plików i folderów.

D. Zaimplementuj ograniczenia kont użytkowników w zasadach grupy.

64. Podczas testu penetracyjnego szarej skrzynki tester odkrywa, że jedna z zapór sieciowych organizacji została skonfigurowana z nazwą użytkownika administratora i hasłem Admin. Tester uzyskuje dostęp administracyjny do zapory i otwiera w niej dziury. Jaki rodzaj luki w uwierzytelnianiu wystąpił w tym scenariuszu?

A. Wykorzystanie słabych danych uwierzytelniających

B. Atak przekierowania

C. Domyślne ustawienia konta exploit

D. brutalne forsowanie poświadczeń

65. Które z poniższych są przykładami exploitów ucieczki w piaskownicy? (Wybierz trzy.)

A. Cold boot attacks

B. Shell upgrade

C. Virtual machine (VM) escape

D. Container escape

E. Ret2libc

F. JTAG debug

66. Utworzyłeś skrypt Bash w swoim katalogu domowym w systemie Linux o nazwie myexploit. Jak możesz to wykonać? (Wybierz dwa.)

A. Wpisz /bin/bash ~/myexploit w wierszu poleceń powłoki.

B. Wpisz myexploit po znaku zachęty powłoki.

C. Wybierz Komputer ➢ Uruchom na pulpicie graficznym; następnie wprowadź ~/

myexploit i wybierz Uruchom.

D. Wpisz run ~/ myexploit po znaku zachęty powłoki.

E. Wpisz chmod u+x ~/ myexploit; następnie wpisz ~/ myexploit po znaku zachęty powłoki.

67. Które polecenie skryptu Bash utworzy nową zmienną o nazwie TOTAL i ustawi jej typ na liczbę całkowitą?

A. variable –i TOTAL

B. declare –i TOTAL

C. declare TOTAL –t integer

D. TOTAL=integer

68. W skrypcie Bash chcesz wysłać standardowe wyjście i standardowy błąd z polecenia tail /var/log/firewall do pliku o nazwie lastevents w bieżącym katalogu. Jakie polecenie możesz dodać do skryptu, aby to zrobić?

A. tail /var/log/firewall 1> lastevents 2> lastevents

B. tail /var/log/firewall > lastevents

C. tail /var/log/firewall 1> lastevents 2> &1

D. tail /var/log/firewall 1&2> lastevents

69. Penetracja chce zaatakować usługę nazw NetBIOS. Które polecenie najprawdopodobniej zostanie użyte do wykorzystania usługi nazw NetBIOS?

A. arpspoof

B. burpsuite

C. nmap

D. respondent

70. Tester penetracyjny chce przeprowadzić zbieranie danych wywiadowczych typu open source (OSINT) z publicznie dostępnych źródeł. Którego z poniższych narzędzi można użyć? (Wybierz dwa.)

A. BeEF

B. Dynamo

C. Maltego

D. SET

E. Shodan

F. Wireshark

71. Podczas pentestu używasz Harvester do prowadzenia pasywnego zbierania informacji w celu gromadzenia adresów e-mail, hostów i nazw domen. Jeśli chciałbyś użyć Shodan do wyszukiwania portów i informacji o usługach dla każdego z zebranych hostów, jakiego przełącznika użyjesz w ramach tej struktury?

A. -b

B. -t

C. -H

D. -h

72. Którego polecenia w Recon-ng można użyć do wyszukania obsługiwanych modułów w ramach frameworka?

A. moduły wyszukiwania

B. moduły pomocy

C. wyszukiwanie

D. pokaż moduły

73. Wszystkie poniższe typy plików (rozszerzenia) są obsługiwane w FOCA oprócz którego?

A. .exe

B . .xls

C. .doc

D. .pdf

E. .sxw

74. Która metoda skanowania portów jest również znana jako półotwarte skanowanie, które nigdy nie nawiązuje prawdziwego połączenia z hostem docelowym przez sieć?

A. TCP scan

B. UDP scan

C. SYN ACK

D. SYN scan

75. Kiedy przeprowadzasz skanowanie portów na celu, która flaga nmap jest używana do określenia zakresu portów?

A. --p

B. -p

C. -Pn

D. -porty

76. Wybierz dwie metody, których możesz użyć do zainstalowania aplikacji innych firm na iDevice po jailbreaku.

A. Sklep z aplikacjami Cydia

B. idb

C. Narzędzie udarowe

D. Sprzęgło

77. Pracownik wysiada z samochodu i zauważa leżący na parkingu dysk USB. Wygląda na to, że dysk jest nowy i ma z boku napis „Moje pliki muzyczne" małą czcionką. Pracownik zabiera dysk do pracy i próbuje odtworzyć jeden z plików muzycznych. Oprogramowanie antywirusowe ostrzega użytkownika o potencjalnym złośliwym oprogramowaniu po tym, jak komputer zaczął zachowywać się nieco dziwnie. Ten rodzaj socjotechniki jest powszechnie znany jako co?

A. Luring

B. Shoulder surfing

C. Waterholing

D. Baiting

78. Social-Engineer Toolkit (SET) to framework oparty na Pythonie, który może wykonać które z poniższych zadań? (Zaznacz wszystkie pasujące odpowiedzi).

A. Wysyłaj e-maile do celów

B. Skanuj adresy IP

C. Twórz ataki SMS-owe

D. Angażuj się w rozmowy przez Wi-Fi

79. Wiele rodzajów środków zaradczych może pomóc organizacjom przygotować się i złagodzić potencjalne ataki socjotechniczne. Które z poniższych są prawidłowymi środkami zaradczymi w przypadku ataków socjotechnicznych? (Zaznacz wszystkie pasujące odpowiedzi).

A. Trening

B. Kamery

C. Niszczarki

D. Wszystkie powyższe

80. Która flaga polecenia mówi hping3, aby używał losowego adresu IP?

A. --random-source

B. --rand-source

C. -S

D. –S