1. Poproszono Cię o wykonanie testu penetracyjnego dla średniej wielkości organizacji, która sprzedaje online części do motocykli na rynku wtórnym. Jakie jest pierwsze zadanie, które powinieneś wykonać?

A. Zbadaj ofertę produktów organizacji.

B. Określ budżet dostępny na test.

C. Określić zakres testu.

D. Uzyskanie uprawnień do wykonania testu.

2. Zatrudniono konsultanta do wykonania testu penetracyjnego dla organizacji. Celem testu są zastrzeżone dokumenty projektowe organizacji. Celem jest obejście środków bezpieczeństwa i uzyskanie nieuprawnionego dostępu do tych dokumentów. Jaki rodzaj oceny jest przeprowadzany w tym scenariuszu?

A. Ocena obiektywna

B. Ocena oparta na celach

C. Ocena oparta na zgodności

D. Ocena zespołu czerwonego

3. Zatrudniono konsultanta do wykonania testu penetracyjnego dla organizacji z branży medycznej. Celem testu jest ogólnodostępna samoobsługowa witryna internetowa, do której użytkownicy mogą uzyskać dostęp, aby przeglądać swoje karty zdrowia. Celem jest obejście środków bezpieczeństwa i uzyskanie nieuprawnionego dostępu do tych informacji. Jaki rodzaj oceny jest przeprowadzany w tym scenariuszu?

A. Ocena obiektywna

B. Ocena szarej skrzynki

C. Ocena oparta na zgodności

D. Ocena białoskrzynkowa

4. Zatrudniono konsultanta do wykonania testu penetracyjnego dla organizacji z branży medycznej. Celem testu jest ogólnodostępna samoobsługowa witryna internetowa, do której użytkownicy mogą uzyskać dostęp, aby przeglądać swoje karty zdrowia. Tester penetracji uzyskał pełną wiedzę na temat podstawowej sieci organizacji. Jaki rodzaj testu jest przeprowadzany w tym przykładzie?

A. Ocena oparta na celach

B. Ocena czarnoskrzynkowa

C. Ocena obiektywna

D. Ocena białoskrzynkowa

5. W jakim typie testu penetracyjnego tester ma ograniczoną ilość informacji o środowisku docelowym, ale nie ma pełnego dostępu?

A. Ocena szarej skrzynki

B. Ocena czarnoskrzynkowa

C. Ocena oparta na zgodności

D. Ocena białoskrzynkowa

6. Poproszono Cię o wykonanie testu penetracji czarnej skrzynki dla średniej wielkości organizacji, która sprzedaje online importowane motocykle i quady. Na jakim etapie tej oceny prawdopodobnie spędzisz większość czasu?

A. Planowanie i określanie zakresu

B. Gromadzenie informacji i identyfikacja słabych punktów

C. Atakowanie i wykorzystywanie

D. Raportowanie i przekazywanie wyników

7. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji, która sprzedaje importowane motocykle i quady za pośrednictwem swojego sklepu internetowego. Musisz dowiedzieć się, kto jest właścicielem domeny organizacji. Którego narzędzia z zestawu narzędzi do testów penetracyjnych powinieneś użyć?

A. nslookup

B. whois

C. Shodan

D. Maltego

8. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji, która sprzedaje importowaną odzież za pośrednictwem swojego sklepu internetowego. Musisz dowiedzieć się, które adresy IP są powiązane z domeną organizacji. Którego narzędzia z zestawu narzędzi do testów penetracyjnych powinieneś użyć?

A. nslookup

B. whois

C. theHarvester

D. Organizacje pobierające odciski palców ze zgromadzonymi archiwami (FOCA)

9. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji, która sprzedaje importowaną odzież za pośrednictwem swojego sklepu internetowego. Chcesz przeszukiwać wyszukiwarki i inne zasoby, aby znaleźć adresy e-mail, nazwiska pracowników i inne szczegóły dotyczące celu. Którego narzędzia z zestawu narzędzi do testów penetracyjnych powinieneś użyć?

A. nmap

B. Shodan

C. theHarvester

D. Organizacje pobierające odciski palców ze zgromadzonymi archiwami (FOCA)

10. Przeprowadzasz test penetracyjny czarnej skrzynki dla dużej organizacji, która zajmuje się sprzedażą hurtową importowanych urządzeń elektronicznych w Stanach Zjednoczonych. Musisz odkryć wszelkie informacje o organizacji, które możesz znaleźć, korzystając z inteligencji typu open

source (OSINT). Którego narzędzia z zestawu narzędzi do testów penetracyjnych możesz użyć, aby to zrobić?

A. Censys

B. whois

C. rekon-ng

D. Shodan

E. Wszystkie powyższe

11. Przeprowadzasz dla klienta test penetracji czarnej skrzynki. Użyłeś narzędzi rozpoznawczych do stworzenia listy adresów e-mail pracowników w organizacji docelowej. Tworzysz wiadomość e-mail adresowaną do wszystkich pracowników, ostrzegającą ich, że muszą zmienić hasło w ciągu 24 godzin, w przeciwnym razie utracą dostęp. Po kliknięciu łącza podanego w wiadomości e-mail zostają przekierowani do Twojej witryny internetowej, gdzie ich poświadczenia są przechwytywane do pliku tekstowego. Jakiego rodzaju exploita użyłeś?

A. Phishing

B. Vishing

C. Smishing

D. Whaling

12. Przeprowadzasz test penetracyjny w szarej skrzynce dla organizacji średniej wielkości. Użyłeś technik rozpoznania, aby zidentyfikować pracownika działu pomocy technicznej i pracownika ds. płac. Tworzysz wiadomość e-mail do pracownika ds. Płac, która wydaje się pochodzić od pracownika działu pomocy, który polecił pracownikowi ds. Płac zresetować hasło. Kiedy kliknie link podany w e-mailu, zostanie przekierowany do Twojej witryny internetowej, gdzie jej poświadczenia są przechwytywane do pliku tekstowego. Jakiego rodzaju exploita użyłeś?

A. Phishing

B. Interrogation

C. Phishing typu spear

D. Whaling

13. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji. Użyłeś technik rozpoznania, aby zidentyfikować adres e-mail dyrektora generalnego, a także adres e-mail należący do pracownika działu pomocy technicznej. Tworzysz wiadomość e-mail do dyrektora generalnego, która wydaje się pochodzić od pracownika działu pomocy technicznej, który polecił dyrektorowi generalnemu zresetowanie hasła. Kiedy kliknie link podany w e-mailu, zostanie przekierowany do Twojej witryny internetowej, gdzie jej poświadczenia są przechwytywane do pliku tekstowego. Jakiego rodzaju exploita użyłeś?

A. Smishing

B. Vishing

C. Phishing typu spear

D. Whaling

14. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji sprzedającej importowaną odzież. Użyłeś technik rozpoznania, aby zidentyfikować kluczowego programistę. Wysyłasz temu pracownikowi spersonalizowaną wiadomość tekstową zawierającą Bitly URL wskazujący na Twoją własną stronę internetową, na której przechwytujesz informacje do pliku tekstowego. Jakiego rodzaju exploita użyłeś w tym scenariuszu?

A. Phishing

B. Smishing

C. Vishing

D. Whaling

15. Przeprowadzasz test penetracyjny czarnej skrzynki dla małej organizacji, która zajmuje się sprzedażą hurtową importowanych urządzeń elektronicznych w Stanach Zjednoczonych. Użyłeś technik rozpoznania, aby zidentyfikować numer telefonu recepcjonistki, a także dostawcę drukarek w organizacji. Dzwonisz do tej recepcjonistki, udając przedstawiciela handlowego sprzedawcy. Poproś recepcjonistę o informacje o swoich drukarkach, stacjach roboczych, systemach operacyjnych itd., Aby dowiedzieć się więcej o infrastrukturze sieciowej organizacji. Jakiego rodzaju exploita użyłeś w tym scenariuszu?

A. Smishing

B. Vishing

C. Phishing typu spear

D. Whaling

16. Przeprowadzasz dla klienta test penetracji szarej skrzynki. Zidentyfikowałeś hosta wewnętrznego z adresem IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie portu SYN tego hosta. Którego polecenia należy użyć, aby to zrobić?

A. nmap 192.168.1.1 -sS

B. nmap 192.168.1.1 -sT

C. nmap 192.168.1.1 -sU

D. nmap 192.168.1.1 -sA

17. Przeprowadzasz dla klienta test penetracyjny typu white box. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie każdego hosta w podsieci 192.168.1.0 (która używa maski podsieci 255.255.255.0). Jakich poleceń możesz użyć, aby to zrobić? (Wybierz dwa.)

A. nmap 192.168.1.0

B. nmap 192.168.1.0-255

C. nmap 192.168.1.0 –m: 255.255.255.0

D. nmap 192.168.1.0/24

E. nmap 192.168.1.1-254

18. Przeprowadzasz dla klienta test penetracyjny w postaci szarej skrzynki. Zidentyfikowałeś hosta wewnętrznego z adresem IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie portu SYN tego hosta. Jakich poleceń możesz użyć, aby to zrobić? (Wybierz dwa.)

A. nmap 192.168.1.1 –sS

B. nmap 192.168.1.1

C. nmap 192.168.1.1 -sV

D. nmap 192.168.1.1 -O

E. nmap 192.168.1.1 –T0

19. Przeprowadzasz dla klienta test penetracyjny w postaci szarej skrzynki. Zidentyfikowałeś hosta wewnętrznego z adresem IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby określić system operacyjny działający na tym hoście. Którego polecenia należy użyć, aby to zrobić?

A. nmap 192.168.1.1 –sS

B. nmap 192.168.1.1 –sL

C. nmap 192.168.1.1 -sV

D. nmap 192.168.1.1 -O

20. Przeprowadzasz dla klienta test penetracyjny. Zidentyfikowałeś hosta wewnętrznego o adresie IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby określić system operacyjny działający na tym hoście. Którego polecenia możesz użyć, aby to zrobić?

A. nmap 192.168.1.1 –A

B. nmap 192.168.1.1 –T1

C. nmap 192.168.1.1 -sT

D. nmap 192.168.1.1 -f

21. Właśnie ukończyłeś test penetracyjny dla klienta. Podczas testu używałeś różnych narzędzi do zbierania danych i przeprowadzania exploitów. Teraz musisz zagregować wszystkie dane wygenerowane przez te narzędzia w spójnym, skorelowanym i czytelnym formacie. Jak nazywa się ten proces?

A. Poświadczenie ustaleń

B. Normalizacja danych

C. Deeskalacja

D. Konflikt

22. Właśnie ukończyłeś test penetracyjny dla klienta i teraz tworzysz pisemny raport ze swoich ustaleń. Musisz upewnić się, że czytelnik rozumie, że podczas przeprowadzania testu postępowałeś zgodnie ze standardem PCI DSS. W której części raportu należy zawrzeć te informacje?

A. Ustalenia

B. Remediacja

C. Metryki i miary

D. Metodologia

23. Jednym z celów komunikacji między testerem a klientem podczas testu penetracyjnego jest zapewnienie, że obie strony jasno rozumieją aktualny stan bezpieczeństwa sieci. Które z poniższych terminów najlepiej opisuje to wspólne zrozumienie?

A. Świadomość sytuacyjna

B. Deeskalacja

C. Dekonflikt

D. Zmiana priorytetów celów

24. Podczas testu penetracyjnego administrator sieci organizacji klienckiej wykrywa atak rozproszonej odmowy usługi (DDoS), którego celem jest serwer sieciowy firmy. Administrator dzwoni do testera penetracji, aby sprawdzić, czy atak jest częścią testu penetracji i nie pochodzi od prawdziwego napastnika. Jak nazywa się ten proces?

A. Normalizacja danych

B. Świadomość sytuacyjna

C. Dekonflikt

D. Zmiana priorytetów celów

25. Podczas testu penetracyjnego organizacja klienta zaczyna otrzymywać skargi od klientów wskazujące, że serwer sieciowy organizacji bardzo wolno reaguje, a czasami nawet ulega awarii. Administrator sieci wykrywa atak rozproszonej odmowy usługi (DDoS), którego celem jest serwer sieciowy firmy. Traci się sprzedaż, więc administrator dzwoni do testera penetracji i prosi o powstrzymanie ataku. Jak nazywa się ta ścieżka komunikacji?

A. Świadomość sytuacyjna

B. Deeskalacja

C. Dekonflikt

D. Zmiana priorytetów celów

26. Niedawno zhakowano sieć organizacji. Osoby atakujące najpierw naruszyły słabe zabezpieczenia używane przez jednego z kontrahentów organizacji. Następnie wykorzystali dane uwierzytelniające kontrahenta, aby uzyskać dostęp do samej organizacji. Jaki rodzaj oceny penetracji mógł temu zapobiec?

A. Oparte na celach

B. Przed połączeniem

C. Oparte na celach

D. Łańcuch dostaw

27. Pracujesz w zespole ds. bezpieczeństwa dużej organizacji. Twój zespół otrzymał zadanie przeprowadzenia wewnętrznego testu penetracyjnego, aby zweryfikować, czy personel IT Twojej organizacji jest w stanie odpowiednio się przed nim obronić. Jaki rodzaj oceny jest używany w tym scenariuszu?

A. Oparte na celach

B. Oparte na zgodności

C. Łańcuch dostaw

D. Drużyna czerwona

28. Która z poniższych kategorii przeciwników klasyfikuje podmioty zagrażające, ogólnie rzecz biorąc, od najmniej groźnych do najbardziej groźnych?

A. Script kiddie, haktywista, złośliwy informator, zorganizowana przestępczość, państwo narodowe

B. Script kiddie, złośliwy insider, haktywista, przestępczość zorganizowana, państwo narodowe

C. Haktywista, script kiddie, złośliwy insider, państwo narodowe, przestępczość zorganizowana

D. Państwo narodowe, przestępczość zorganizowana, złośliwy insider, haktywista, script kiddie

29. Jednym z Twoich klientów jest publiczna grupa rzecznicza. Niektóre z jej poglądów politycznych są bardzo niepopularne wśród kilku marginalnych aktywistów i obawiają się, że haktywista może próbować przejąć dostępną publicznie stronę internetową. Poprosili cię o przeprowadzenie testu penetracyjnego przy użyciu tych samych narzędzi i technik, które typowy haktywista miałby techniczne umiejętności i środki do wykorzystania. Jaki proces miał miejsce w tym scenariuszu?

A. Należyta staranność

B. Akceptacja ryzyka

C. Modelowanie zagrożeń

D. Pełzanie zakresu

30. Spotykasz się z nowym klientem, aby określić parametry przyszłego testu penetracyjnego. W trakcie rozmowy pytasz klienta, czy jest skłonny zaakceptować fakt, że test penetracyjny może spowodować zakłócenia w świadczeniu usług w jego organizacji. Klient odpowiada twierdząco. Jaki proces miał miejsce w tym scenariuszu?

A. Akceptacja ryzyka

B. Należyta staranność

C. Modelowanie zagrożeń

D. Przeniesienie ryzyka

31. W ramach procesu zbierania informacji podczas testu penetracyjnego szarej skrzynki należy przeprowadzić kontrolę certyfikatu na wewnętrznym serwerze sieciowym organizacji docelowej. Którego narzędzia możesz użyć na swoim laptopie Kali Linux, aby to zrobić?

A. sslyze

B. Zenmap

C. nmap

D. hping

32. Podczas testu penetracyjnego szarej skrzynki użyłeś narzędzia na swoim laptopie Kali Linux, aby sprawdzić certyfikat używany przez wewnętrzny serwer sieciowy organizacji docelowej. Wynik jest pokazany tutaj:

```
* SSLV2 Cipher Suites:
    Server rejected all cipher suites.

* TLSV1_2 Cipher Suites:
    Preferred:
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
              ECDHE-RSA-AES256-SHA384       ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA256         DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA            DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-GCM-SHA384     DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA256-SHA               -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA256                 -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA                    -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-GCM-SHA384             -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA256       ECDH-256 bits  128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA256         DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA            DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-GCM-SHA256     DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA128-SHA               -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA256                 -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA                    -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-GCM-SHA256             -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1_1 Cipher Suites:
    Preferred:
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA            DH-2048 bits   256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA256-SHA               -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA                    -              256 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA            DH-2048 bits   128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA128-SHA               -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA                    -              128 bits     HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1 Cipher Suites:
    Server rejected all cipher suites.

* SSLV3 Cipher Suites:
    Server rejected all cipher suites.
```

Czego możesz się nauczyć z tego wyniku? (Wybierz dwa.)

A. SSLv2 jest obsługiwany przez serwer WWW.

B. TLSv1_1 jest obsługiwany przez serwer WWW.

C. TLSv1_2 jest obsługiwany przez serwer WWW.

D. TLSv1 jest obsługiwany przez serwer WWW.

E. SSLv3 jest obsługiwany przez serwer WWW.

33. Musisz przechwycić pakiety w sieci przewodowej podczas fazy zbierania informacji testu penetracyjnego szarej skrzynki. Jakich narzędzi możesz użyć na swoim laptopie, aby to osiągnąć? (Wybierz dwa.)

A. tcpdump

B. nmap

C. Wireshark

D. Zenmap

E. aircrack-ng

34. Podczas fazy zbierania informacji w teście penetracji czarnej skrzynki musisz podsłuchiwać emisje o częstotliwości radiowej pochodzące z obiektu celu i próbować przechwycić dane z jego sieci bezprzewodowej. Zanim to zrobisz, musisz złamać szyfrowanie używane w sieci Wi-Fi. Jesteś zaparkowany na parkingu organizacji. Którego narzędzia możesz użyć na swoim laptopie z systemem Linux, aby to zrobić?

A. aircrack-ng

B. tcpdump

C. Wireshark

D. nmap

35. Podczas fazy zbierania informacji w teście penetracyjnym czarnej skrzynki musisz podsłuchiwać emisje o częstotliwości radiowej pochodzące z obiektu celu i próbować przechwycić dane z jego sieci bezprzewodowej. Jesteś zaparkowany na parkingu organizacji. Jak należy skonfigurować interfejs sieci bezprzewodowej w laptopie, aby to zrobić?

A. Ustaw tryb monitorowania.

B. Ustaw na tryb bezładny.

C. Ustaw tryb przechwytywania.

D. Ustaw tryb IEEE 802.1x.

36. Tester penetracyjny podszywa się pod osobę zajmującą się naprawą ogrzewania i chłodzenia, aby uzyskać fizyczny dostęp do obiektu organizacji docelowej. Po wejściu do środka prosi o dostęp do serwerowni w celu zbadania problemu z powrotem zimnego powietrza. Opuszczając serwerownię, ukradkiem umieszcza w otworze drzwi mały drewniany klin, uniemożliwiając całkowite zamknięcie drzwi. Dzięki temu może później wrócić do pokoju bez zezwolenia. Jak nazywa się ta technika?

A. Otwieranie zamków

B. Zablokuj obejście

C. Skakanie przez płot

D. Klonowanie odznak

37. Którą z poniższych funkcji czujnika wyjścia można manipulować, aby umożliwić penetratorowi wejście do budynku bez autoryzacji?

A. Awaryjne otwieranie awaryjne

B. Automatyczne blokowanie

C. Automatyczne odblokowanie za pomocą czujnika ruchu dla wyjścia

D. Automatyczne odblokowanie za pomocą czujnika światła do wyjścia

38. Tester penetracyjny grzebie w śmieciach organizacji docelowej i znajduje wyrzuconą odznakę dostępu. Replikuje nową odznakę ze swoim zdjęciem, używając odrzuconej odznaki jako modelu. Używa urządzenia do odczytania paska magnetycznego wyrzuconej odznaki i powielenia go na fałszywej odznace. Jakie techniki zostały użyte przez testera w tym scenariuszu? (Wybierz dwa.)

A. Otwieranie zamków

B. Nurkowanie w śmietniku

C. Skakanie przez płot

D. Klonowanie odznak

E. Zablokuj obejście

39. Korzystając z rozpoznania, tester penetracyjny dowiaduje się, że pracownicy organizacji docelowej używają identyfikatorów dostępu RFID do otwierania drzwi w obiekcie. Korzystając ze strony internetowej firmy, identyfikuje pracowników wysokiego szczebla w organizacji. Potem czeka na parkingu, aż zobaczy jedną z tych osób zmierzającą w stronę drzwi wejściowych. Wchodzi za nimi do recepcji z małym czytnikiem RFID ukrytym w płaszczu. Przechwytuje podpis RFID z identyfikatora osoby, a następnie tworzy własną fałszywą identyfikator dostępu i koduje ją tym podpisem RFID. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

40. Penetracja przeprowadza dla klienta test szarej skrzynki. Podczas skanowania sieci zauważa host, który ma otwarty port TCP 139. Podejrzewa, że jest to system Windows, więc uruchamia polecenie NBTSTAT i odkrywa kluczowe informacje o hoście. Który protokół na zdalnym hoście umożliwił testerowi zebranie tych informacji?

A. NetBIOS

B. SNMP

C. NAC

D. SMTP

41. W ramach testu penetracyjnego musisz przeprowadzić rozpoznanie docelowej organizacji, aby pasywnie zebrać informacje. Jakich narzędzi możesz do tego użyć? (Wybierz dwa.)

A. whois

B. Framework Metasploit

C. OpenVAS

D. nslookup

E. Nessusa

42. W ramach testu penetracyjnego musisz nawiązać aktywne połączenie z systemami komputerowymi i urządzeniami w organizacji docelowej, aby je wyliczyć i odciskać palcami. Jakich narzędzi możesz do tego użyć? (Wybierz dwa.)

A. whois

B. nmap

C. hping

D. Aircrack-ng

E. John the Ripper

43. W ramach testu penetracyjnego musisz zebrać nazwy kont użytkowników i hasła z plików passwd i shadow z serwera Linux. Jakich narzędzi możesz do tego użyć? (Wybierz dwa.)

A. John the Ripper

B. Kain i Abel

C. Kismet

D. Censys

E. Rozpoznanie

44. W ramach testu penetracyjnego musisz wykonać dogłębne skanowanie celu w celu zidentyfikowania luk, takich jak brakujące aktualizacje lub źle skonfigurowane ustawienia zabezpieczeń. Jakich narzędzi możesz do tego użyć?

A. Censys

B. Kombajn

C. Shodan

D. OWASP ZAP

E. Nessusa

45. Penetracja przeprowadza dla klienta test szarej skrzynki. Tester postanawia przeprowadzić atak brute-force na bazę danych SQL. Jakiego narzędzia można do tego użyć?

A. John the Ripper

B. Mapa SQL

C. WiFite

D. Nikto

46. Właśnie zakończyłeś test penetracyjny dla klienta. Klient zatrudnia ponad 2000 pracowników, ale tylko dwóch z nich to administratorzy sieci. Podczas testu udało ci się szybko przytłoczyć ich ilością swoich ataków. Aby wyeliminować tę lukę, zaleca się, aby klient zatrudnił dodatkowych administratorów sieci, którzy mają poświadczenia i doświadczenie w zakresie cyberbezpieczeństwa. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

47. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu odkryłeś, że pracownicy organizacji intensywnie korzystają z udostępnionego konta Dysku Google do współpracy. Udało Ci się użyć exploita socjotechnicznego, aby uzyskać dostęp do współdzielonego konta i uzyskać dostęp do poufnych plików. Aby wyeliminować tę lukę, zaleca się, aby klient nie zezwalał na takie praktyki wśród pracowników. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

48. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu udało Ci się uzyskać dostęp do fizycznego obiektu klienta, śledząc grupę pracowników. Aby wyeliminować tę lukę, zaleca się, aby klient zaimplementował drzwi z pułapką na ludzi przy wejściu do obiektu. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

49. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu uzyskałeś dostęp do sieci bezprzewodowej klienta za pomocą Aircrackng, siedząc w samochodzie na parkingu po drugiej stronie ulicy. Aby wyeliminować tę lukę, zaleca się, aby klient zaimplementował kierunkowe anteny sieci bezprzewodowej, a także manipulował poziomem mocy punktów dostępu, aby zapobiec emanacji sygnału. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

50. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu udało Ci się wykorzystać socjotechnikę, aby przekonać pracownika obsługi rachunków organizacji do wysłania dużej płatności ACH na fikcyjne konto bankowe. Aby wyeliminować tę lukę, zaleca się, aby klient zaimplementował podział obowiązków w taki sposób, aby dwie osoby musiały podpisać się na wszystkie wypłaty. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

51. Jesteś CIO średniej wielkości korporacji. Opracowujesz plan wdrożenia regularnych testów penetracyjnych i rozważasz skorzystanie z wewnętrznego zespołu testów penetracyjnych składającego się z własnych pracowników. Które z poniższych są korzyściami płynącymi z korzystania z wewnętrznego zespołu? (Wybierz dwa.)

A. Posiadają kontekstową wiedzę o organizacji.

B. Są mniej stronniczy niż zewnętrzny wykonawca.

C. Posiada niezależność wymaganą do przeprowadzenia dokładnego testu.

D. Mają dogłębne doświadczenie w przeprowadzaniu testów penetracyjnych dla wielu organizacji.

E. Zwykle jest to tańsze niż korzystanie z usług zewnętrznego wykonawcy.

52. Jesteś CIO średniej wielkości korporacji. Opracowujesz plan wdrożenia regularnych testów penetracyjnych i rozważasz skorzystanie z zewnętrznego wykonawcy testów penetracyjnych. Które z poniższych są korzyściami płynącymi z korzystania z zespołu zewnętrznego? (Wybierz dwa.)

A. Posiadają kontekstową wiedzę o organizacji.

B. Są mniej stronniczy niż zespół wewnętrzny.

C. Posiada niezależność wymaganą do przeprowadzenia dokładnego testu.

D. Są dokładnie zaznajomieni z mechanizmami kontroli bezpieczeństwa w organizacji.

E. Zwykle jest to tańsze niż korzystanie z wewnętrznego zespołu.

53. Jesteś CIO średniej wielkości korporacji. Opracowujesz plan wdrożenia regularnych testów penetracyjnych i rozważasz skorzystanie z wewnętrznego zespołu testów penetracyjnych składającego się z własnych pracowników. Które z poniższych są wadami korzystania z zespołu wewnętrznego? (Wybierz dwa.)

A. Utrzymanie wewnętrznego zespołu jest bardzo kosztowne.

B. Istnieje potencjalny konflikt interesów, jeśli przeprowadzają również testy dla jednego z Twoich konkurentów.

C. Mogą mieć wrażenie, że wykryta luka może źle na nich odbijać.

D. Mogą brakować obiektywizmu.

54. Jesteś CIO średniej wielkości korporacji. Opracowujesz plan wdrożenia regularnych testów penetracyjnych i rozważasz skorzystanie z zewnętrznego wykonawcy testów penetracyjnych. Które z poniższych są wadami korzystania z zespołu zewnętrznego? (Wybierz dwa.)

A. Istnieje potencjalny konflikt interesów, jeśli przeprowadzają oni również testy dla jednego z Twoich konkurentów.

B. Brakuje im talentu technicznego wewnętrznego zespołu.

C. Zazwyczaj są droższe niż zespół wewnętrzny.

D. Mogą poddać testowi swoje osobiste uprzedzenia.

55. Które z poniższych najlepiej opisuje pojęcie nastawienia hakera w kontekście testów penetracyjnych?

A. Tester penetracyjny musi przyjąć defensywne nastawienie, starając się chronić przed wszystkimi zagrożeniami.

B. Tester penetracyjny musi myśleć jak profesjonalista ds. bezpieczeństwa, oceniając siłę i wartość każdej używanej kontroli bezpieczeństwa.

C. Tester penetracyjny musi myśleć jak przeciwnik, który może zaatakować system w prawdziwym świecie.

D. Tester penetracji musi myśleć jak dowódca wojskowy, organizując otwarty atak na wielu frontach przez wielu napastników.

56. Przeprowadzasz test penetracji szarej skrzynki. Musisz uruchomić skanowanie podatności na wrażliwy wewnętrzny system serwera? Jak skonfigurować skanowanie?

A. Użyj opcji –T5 z poleceniem nmap.

B. Użyj opcji –T3 z poleceniem nmap.

C. Użyj opcji –T2 z poleceniem nmap.

D. Użyj opcji –T0 z poleceniem nmap.

57. Które z poniższych kwestii mogą być konieczne do rozważenia podczas wykonywania skanowania luk w zabezpieczeniach w organizacji, która uruchamia aplikacje sieciowe w kontenerach? (Wybierz dwa.)

A. Aplikacje działające w środowisku kontenera mogą nie być wykrywane przez tradycyjne skanowanie luk w zabezpieczeniach.

B. Hosty kontenerów mogą spowolnić skanowanie luk w zabezpieczeniach.

C. Skanowanie hosta kontenera może spowodować awarię aplikacji działających w jego kontenerach.

D. Skanowanie hosta kontenera może spowodować jego awarię, powodując przełączenie krytycznych aplikacji sieciowych do trybu offline.

E. Podatności związane z podstawowym systemem operacyjnym hosta kontenera mogą być dziedziczone przez jego kontenery.

58. Która z poniższych technik skanowania aplikacji jest wykonywana poprzez przeglądanie kodu źródłowego aplikacji?

A. Statyczna analiza kodu

B. Dynamiczna analiza kodu

C. Fuzzing

D. Żadne z powyższych

59. Które z poniższych technik skanowania aplikacji są wykonywane na uruchomionych aplikacjach? (Wybierz dwa.)

A. Statyczna analiza kodu

B. Dynamiczna analiza kodu

C. Fuzzing

D. Analiza kodu źródłowego

60. Która z poniższych technik skanowania aplikacji polega na wysyłaniu losowych, nieoczekiwanych lub nieprawidłowych danych do wejść aplikacji w celu sprawdzenia, jak reaguje?

A. Statyczna analiza kodu

B. Fuzzing

C. Analiza kodu źródłowego

D. Żadne z powyższych

61. Tester penetracyjny podszywa się pod osobę zajmującą się naprawą automatów sprzedających, aby uzyskać dostęp do obiektu organizacji docelowej. W środku tester ukrywa urządzenie bezprzewodowe za automatem sprzedającym, które przechwytuje sygnał radiowy sieci bezprzewodowej organizacji i ponownie nadaje go z dużym wzmocnieniem w kierunku parkingu. Jaki exploit sieci bezprzewodowej wykorzystał tester w tym scenariuszu?

A. Atak karmy

B. Powtarzający się atak

C. Atak downgrade

D. Atak zagłuszający

62. Tester penetracyjny poszukuje luk w zabezpieczeniach aplikacji internetowej używanej przez docelową organizację. Na stronie logowania wpisuje w polu Hasło następujący ciąg tekstowy: UNION SELECT Nazwa użytkownika, Hasło FROM Użytkownicy; Jaki rodzaj exploita jest używany w tym przykładzie?

A. Wstrzyknięcie SQL

B. Wstrzyknięcie HTML

C. Wstrzyknięcie polecenia

D. Wstrzyknięcie kodu

63. Tester penetracyjny przegląda konta w mediach społecznościowych należące do CIO organizacji docelowej i sporządza listę możliwych haseł, takich jak imię i nazwisko współmałżonka, imię zwierzaka, ulubione drużyny sportowe i tak dalej. Tester próbuje zalogować się na konto CIO za pomocą jednego możliwego hasła po drugim, próbując znaleźć takie, które działa. Jaki to rodzaj exploita uwierzytelniania?

A. brutalne forsowanie poświadczeń

B. Przejmowanie sesji

C. Atak przekierowania

D. Łamanie hasła

64. Podczas testu penetracyjnego szarej skrzynki tester używa Wireshark do sniffowania ruchu sieciowego między przeglądarką pracownika a stroną internetową i jest w stanie przechwycić plik cookie sesji. Tester jest wtedy w stanie podszywać się pod ofiarę bez przechwytywania rzeczywistych danych uwierzytelniających użytkownika. Jaki typ luki w uwierzytelnianiu został użyty w tym scenariuszu?

A. Eksploat Kerberos

B. Przejmowanie sesji

C. Atak przekierowania

D. Łamanie hasła

65. Podczas testu penetracyjnego szarej skrzynki tester wykorzystuje wiadomości phishingowe do wysyłania użytkowników do strony logowania, która wygląda jak strona samoobsługi zasobów ludzkich organizacji docelowej. Fałszywa strona służy do przechwytywania danych uwierzytelniających pracowników. Jaki typ luki w uwierzytelnianiu został użyty w tym scenariuszu?

A. Eksploat Kerberos

B. Przejmowanie sesji

C. Atak przekierowania

D. brutalne wymuszanie uwierzytelnienia

66. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt Bash, aby uruchomić exploita przeciwko docelowej organizacji. Jako część skryptu musisz wstawić wartość FS1 do elementu o nazwie HostName w tablicy asocjacyjnej o nazwie Target. Który z poniższych wierszy kodu to zrobi?

A. Cel [Nazwa Hosta] = FS1

B. Cel = [{"HostName":"FS1"}]

C. $Target.HostName = 'FS1'

D. _Cel = {"Nazwa Hosta" => "FS1"}

67. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt Ruby, aby uruchomić exploita przeciwko docelowej organizacji. Jako część skryptu musisz wstawić wartość FS1 do elementu o nazwie HostName w tablicy asocjacyjnej o nazwie Target. Który z poniższych wierszy kodu to zrobi?

A. Cel [Nazwa Hosta] = FS1

B. Cel = [{"HostName":"FS1"}]

C. $Target.HostName = 'FS1'

D. _Cel = {"Nazwa Hosta" => "FS1"}

68. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt PowerShell, aby uruchomić exploita przeciwko docelowej organizacji. Jako część skryptu musisz wstawić wartość FS1 do elementu o nazwie HostName w tablicy asocjacyjnej o nazwie Target. Który z poniższych wierszy kodu to zrobi?

A. Cel [Nazwa Hosta] = FS1

B. Cel = [{"HostName":"FS1"}]

C. $Target.HostName = 'FS1'

D. _Cel = {"Nazwa Hosta" => "FS1"}

69. W ramach testu penetracyjnego szarej skrzynki musisz stworzyć skrypt Pythona, aby uruchomić exploita przeciwko docelowej organizacji. Jako część skryptu musisz wstawić wartość FS1 do elementu o nazwie HostName w tablicy asocjacyjnej o nazwie Target. Który z poniższych wierszy kodu to zrobi?

A. Cel [Nazwa Hosta] = FS1

B. Cel = [{"HostName":"FS1"}]

C. $Target.HostName = 'FS1'

D. _Cel = {"Nazwa Hosta" => "FS1"}

70. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt Ruby, aby uruchomić exploita przeciwko docelowej organizacji. W ramach skryptu musisz dokonać porównania między dwiema zmiennymi, aby sprawdzić, czy są sobie równe. Którego operatora relacji powinieneś użyć?

A. =

B. ==

C. -eq

D. !=

71. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu odkryłeś, że jeden z administratorów systemu Linux używa usługi Telnet do zdalnego dostępu do serwerów Linux. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem?

A. Zabroń dostępu do serwera zdalnego.

B. Użyj SFTP do zdalnego dostępu do serwera.

C. Użyj rsh do zdalnego dostępu do serwera.

D. Użyj SSH do zdalnego dostępu do serwera.

72. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu odkryłeś, że jeden z administratorów systemu Linux używa rcp do kopiowania plików między serwerami Linux. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem?

O. Użyj polecenia scp do przesyłania plików.

B. Zabroń przesyłania plików między serwerami.

C. Użyj polecenia rsh do przesyłania plików.

D. Użyj polecenia ftp do przesyłania plików.

73. Właśnie zakończyłeś test penetracyjny szarej skrzynki dla klienta. Podczas testu uzyskałeś dostęp do kontrolera sieci bezprzewodowej organizacji przy użyciu domyślnej nazwy użytkownika i hasła administratora. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem?

A. Wyeliminuj transmisję haseł w postaci zwykłego tekstu, używając protokołu SSH do połączeń zdalnych.

B. Zmień domyślną nazwę użytkownika i hasło administratora na kontrolerze.

C. Użyj anten kierunkowych we wszystkich punktach dostępowych.

D. Zaimplementuj filtrowanie adresów MAC w sieci bezprzewodowej.

74. Właśnie zakończyłeś test penetracji czarnej skrzynki dla klienta. Sieć bezprzewodowa organizacji korzysta z kluczy wstępnych. Podczas testu uzyskałeś dostęp do sieci bezprzewodowej organizacji z parkingu za pomocą laptopa z systemem Aircrack-ng. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem? (Wybierz dwa.)

A. Zaimplementuj filtrowanie adresów MAC.

B. Zaimplementuj uwierzytelnianie 802.1x.

C. Zaktualizuj do nowszego sprzętu Wi-Fi, który obsługuje nowoczesne metody szyfrowania.

D. Zmień domyślną nazwę użytkownika i hasło administratora w punkcie dostępowym.

E. Skonfiguruj ponownie sprzęt Wi-Fi, aby korzystał z szyfrowania WPA.

75. Właśnie zakończyłeś test penetracji czarnej skrzynki dla klienta. Podczas testu uzyskałeś dostęp do sieci bezprzewodowej organizacji z parkingu za pomocą laptopa z systemem Aircrack-ng. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem? (Wybierz dwa.)

A. Użyj anten kierunkowych we wszystkich punktach dostępowych.

B. Ponownie skonfiguruj sprzęt Wi-Fi, aby korzystał z szyfrowania WEP.

C. Zaktualizuj do nowszego sprzętu Wi-Fi, który obsługuje nowoczesne metody szyfrowania.

D. Wyłącz DHCP w sieci bezprzewodowej.

76. Udało Ci się pomyślnie zamontować udział NFS w sieci z ograniczonymi uprawnieniami. Przeglądając sieciowy system plików, zauważysz, że pliki i katalogi nie pokazują nazwy właściciela lub grupy plików i katalogów. Jaka jest prawdopodobna tego przyczyna?

A. Nie montujesz systemu plików z uprawnieniami roota, więc Twój system nie może zinterpretować wartości UID.

B. System plików NFS nie jest poprawnie skonfigurowany, co oznacza, że prawdopodobnie możesz wykorzystać tę słabość.

C. Wartości UID i GID przypisane do plików i katalogów w udziale NFS nie są mapowane na host lokalny.

D. Serwer NFS wie tylko, że UID 0 jest mapowany na konto root. Jeśli utworzysz konto na lokalnym hoście z wartością UID jednego z plików NFS, serwer NFS nie będzie już mógł odczytać tego pliku.

77. Do czego można wykorzystać otwarte serwery przekazujące pocztę z włączonymi VRFY i EXPN, które umożliwiają anonimowym użytkownikom łączenie się? (Zaznacz wszystkie pasujące odpowiedzi).

A. Wymień ważne konta użytkowników

B. Wyślij e-mail na wewnętrzne adresy e-mail

C. Wyślij e-mail na zewnętrzne adresy e-mail

D. Określ wersję systemu operacyjnego hosta docelowego

78. Zło bliźniaczy punkt dostępowy to rodzaj ataku używany do powielania istnienia legalnego punktu dostępowego w celu zachęcenia ofiar do łączenia się w celu atakowania urządzeń lub komunikacji użytkowników końcowych. Innym sposobem na naśladowanie wszystkich możliwych punktów dostępu z żądań sygnałów nawigacyjnych klienta jest nazwane co?

A. Atak karmy

B. Powtórz atak

C. Powtórka ataku AP

D. Atak socjotechniczny

79. To polecenie może być użyte do wykonania typu „ping of death" na urządzeniach Bluetooth.

A. L2PP

B. L2TP

C. L2PING

D. LPING

80. Wszystkie poniższe warstwy są warstwami w stosie protokołów Bluetooth, z wyjątkiem której?

A. LMP

B. SDP

C. L2CAP

D.TC2

E. RCOMM