1. 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 są niedostępne podczas testu. Co zrobiłeś niepoprawnie w tym scenariuszu?

A. Cel powinien mieć możliwość użycia dowolnych środków do obrony.

B. Posiadanie szczegółowych informacji o sieci wewnętrznej unieważnia wyniki testu.

C. Testowaniu powinny podlegać wszystkie zasoby sieciowe, w tym zasoby w chmurze.

D. Nic. ROE zostało odpowiednio zdefiniowane.

2. Określasz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Będzie to ocena z czarnej skrzynki. Klient określił, że nie chce, aby test był przeprowadzany w godzinach szczytu dnia, więc do dokumentu dodano ramy czasowe „przekroczenia" czasu, kiedy testowanie zostanie zawieszone. Określiłeś, że żadna komunikacja między Tobą a klientem nie będzie się odbywać do końca testu, kiedy prześlesz ostateczne wyniki testu. Określiłeś również, że cel musi zapewniać wewnętrzny dostęp do sieci, mapę sieci i poświadczenia uwierzytelniania. Co zrobiłeś źle w tym scenariuszu?

A. Posiadanie szczegółowych informacji o sieci wewnętrznej unieważnia wyniki testu.

B. Wstrzymanie oceny w godzinach szczytu unieważnia wyniki testu.

C. Komunikacja między testerami a klientem powinna odbywać się w regularnych odstępach czasu przez cały czas trwania testu.

D. Nic. ROE zostało odpowiednio zdefiniowane.

3. Jesteś właścicielem małej firmy konsultingowej zajmującej się testami penetracyjnymi. Martwisz się, że klient może pozwać Cię miesiące lub lata po zakończeniu testów penetracyjnych, jeśli jego sieć zostanie naruszona przez exploita, który nie istniał w momencie przeprowadzania testu. Co powinieneś zrobić?

A. Nalegaj, aby klienci podpisali umowę o zachowaniu poufności (NDA) przed testem.

B. Dołącz do umowy zastrzeżenie wskazujące, że wyniki są ważne tylko w momencie wykonania testu.

C. Zawrzeć w umowie klauzulę arbitrażową, aby zapobiec procesowi sądowemu.

D. Nalegaj, aby klienci podpisali oświadczenie o pracy (SOW) przed testem.

4. Jesteś właścicielem małej firmy konsultingowej zajmującej się testami penetracyjnymi. Martwisz się, że klient, który żąda oceny czarnej skrzynki, może pozwać Cię po zakończeniu testów penetracyjnych, jeśli jego sieć zostanie naruszona przez exploit. Co powinieneś zrobić?

A. Nalegaj, aby klienci podpisali zamówienie przed testem.

B. Nalegaj, aby przed testem klienci podpisali główną umowę o świadczenie usług (MSA).

C. Dołącz do umowy zastrzeżenie wskazujące, że metodologia testu może wpłynąć na kompleksowość testu.

D. Odmówić wykonania testów czarnoskrzynkowych.

5. Określasz zasady zaangażowania (ROE) w nadchodzącym teście penetracyjnym. Pracujesz w sekcji dokumentu dotyczącej rozwiązywania problemów. Jakie elementy powinny znaleźć się w tej sekcji? (Wybierz dwa.)

A. Jasno określone procedury eskalacji problemów

B. Harmonogram zaangażowania

C. Systemy, aplikacje i dostawcy usług objętych zakresem

D. Systemy, aplikacje i dostawcy usług poza zakresem

E. Potwierdzenie, że testy penetracyjne niosą ze sobą nieodłączne ryzyko

6. Przeprowadzasz rekonesans w ramach testu penetracji szarej skrzynki. Uruchamiasz skanowanie pod kątem luk w zabezpieczeniach na jednym z serwerów docelowej organizacji i odkrywasz, że port 143 jest otwarty. Na co to wskazuje?

A. Jest to serwer LDAP.

B. Jest to serwer pocztowy POP3.

C. Jest to serwer SSH.

D. Jest to serwer pocztowy IMAP.

7. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie pod kątem luk w zabezpieczeniach na jednym z serwerów organizacji docelowej i odkrywasz, że port 22 jest otwarty. Na co to wskazuje?

A. Jest to serwer LDAP.

B. Jest to serwer pocztowy POP3.

C. Jest to serwer SSH.

D. Jest to serwer HTTP.

8. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie podatności na jednym z serwerów docelowej organizacji i odkrywasz, że porty 80 i 443 są otwarte. Na co to wskazuje?

A. Jest to serwer LDAP.

B. Jest to serwer uwierzytelniania Kerberos.

C. Jest to serwer pocztowy POP3.

D. Jest to serwer HTTP.

9. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie podatności na jednym z serwerów docelowej organizacji i odkrywasz, że porty 389 i 636 są otwarte. Na co to wskazuje?

A. Jest to serwer LDAP.

B. Jest to serwer uwierzytelniania Kerberos.

C. Jest to serwer Katalogu Globalnego.

D. Jest to serwer DNS.

10. Przeprowadzasz rekonesans w ramach testu penetracyjnego szarej skrzynki. Uruchamiasz skanowanie pod kątem luk w zabezpieczeniach na jednym z serwerów docelowej organizacji i odkrywasz, że port 53 jest otwarty. Na co to wskazuje?

A. Jest to serwer NTP.

B. Jest to serwer uwierzytelniania Kerberos.

C. Jest to serwer Katalogu Globalnego.

D. Jest to serwer DNS.

11. Przeprowadzasz rekonesans w ramach testu penetracji czarnej skrzynki. Zauważasz, że pracownicy organizacji docelowej często gromadzą się w określonej restauracji na świeżym powietrzu na lunch. Zatrudniasz kilku młodych, atrakcyjnych fizycznie konsultantów do pomocy przy teście penetracyjnym. Wysyłasz ich do tej samej restauracji na lunch i każesz im zaprzyjaźnić się z kilkoma pracownikami docelowej organizacji. Zdobywają zaufanie pracowników, a pracownicy zaczynają dzielić się informacjami o swojej pracy, komputery, szefowie, klienci, projekty i tak dalej. Jaki czynnik motywacyjny został użyty w tym scenariuszu?

A. Władza

B. Niedobór

C. Dowód społeczny

D. Podobieństwo

12. Podczas testu penetracyjnego wysyłasz e-mail do dyrektora finansowego docelowej organizacji. E-mail twierdzi, że kamera internetowa na laptopie dyrektora finansowego została potajemnie wykorzystana do nagrania jego oglądania pornografii. E-mail grozi opublikowaniem tego filmu i powiadomieniem rodziny, pracodawcy i policji, jeśli nie odpowie, podając pewne poufne informacje dotyczące swojej firmy. Jaki czynnik motywacyjny został użyty w tym scenariuszu?

Strach

B. Dowód społeczny

C. Władza

D. Niedobór

13. Tester penetracyjny wysyła wiadomość e-mail do przedstawiciela handlowego docelowej organizacji, podając się za prezesa jednego z najważniejszych klientów organizacji. Wiadomość e-mail prosi pracownika o utworzenie konta VPN, aby umożliwić prezesowi dostęp do określonych plików w sieci organizacji. E-mail grozi zakończeniem relacji biznesowej, jeśli tak się nie stanie. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Podobieństwo

B. Dowód społeczny

C. Władza

D. Niedobór

14. Penetracja wysyła wiadomość e-mail do pracownika docelowej organizacji, podając się za handlowca w trasie. W e-mailu twierdzi, że jej połączenie VPN z hotelu działa bardzo wolno i że nie może uzyskać dostępu do danych klienta. Jeśli nie zdobędzie danych, straci sprzedaż. Wiadomość prosi pracownika o przesłanie jej kopii plików pocztą elektroniczną. Jaki czynnik motywacyjny wykorzystał tester penetracyjny w tym scenariuszu?

A. Dowód społeczny

B. Pośpiech

C. Niedobór

D. Władza

15. Tester penetracyjny wysyła wiadomość e-mail do pracownika docelowej organizacji, podając się za przedstawiciela handlowego w trasie. W e-mailu twierdzi, że zapomniała hasła VPN, a teraz jest ono zablokowane, ponieważ próbowała zbyt wielu błędnych haseł. Prosi pracownika o jego nazwę użytkownika i hasło VPN, aby mogła się zalogować i zaktualizować bazę danych klientów za pomocą nowego ogromnego zamówienia. Wspomina w e-mailu, że jeden ze współpracowników docelowego pracownika zrobił to dla niej w przeszłości i nie była to wielka sprawa. Jakie czynniki motywacyjne wykorzystał tester penetracyjny w tym scenariuszu? (Wybierz dwa.)

A. Dowód społeczny

B. Pośpiech

C. Niedobór

D. Władza

E. Strach

16. Penetracja używa nmapa do skanowania hostów w sieci docelowej. Klient używa agresywnego narzędzia IPS i zatrudnia doświadczony personel IT, którego musi unikać. Jakiej opcji czasu powinna użyć z nmapem, aby uniknąć wykrycia? (Załóżmy, że czas nie jest problemem.)

A. -T1

B. -T3

C. -T4

D. -T5

17. Tester penetracyjny używa nmap do skanowania hostów w sieci docelowej. Klient ma luźną postawę bezpieczeństwa i zatrudnia stosunkowo niedoświadczony personel IT. Którą opcję pomiaru czasu mogłaby rozważyć użycie z nmapem, aby przyspieszyć skanowanie?

A. -T1

B. -T2

C. -T3

D. -T4

18. Tester penetracyjny uruchamia skanowanie nmap bez określania opcji czasu. Który jest używany domyślnie?

A. -T1

B. -T2

C. -T3

D. -T4

E. -T0

19. Która opcja taktowania nmapa powoduje skanowanie w trybie Paranoid?

A. -T0

B. -T1

C. -T2

D. -T3

E. -T4

20. Która opcja taktowania nmapa powoduje, że skanuje w trybie Insane?

A. -T5

B. -T4

C. -T3

D. -T2

E. -T1

21. Generujesz pisemny raport ustaleń po teście penetracyjnym. Podczas testu postępowałeś zgodnie ze standardem NIST 800-115. W której części raportu należy zawrzeć te informacje?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

22. Generujesz pisemny raport ustaleń po teście penetracyjnym. W której części raportu należy przedstawić czytelnikowi streszczenie testu i wyniki na wysokim poziomie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

23. Generujesz pisemny raport ustaleń po teście penetracyjnym. W której sekcji należy zgłosić oceny ryzyka?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

24. Która część pisemnego raportu z wyników testów penetracyjnych jest przeznaczona do przeczytania przez mniej zaawansowaną publiczność?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

25. Generujesz pisemny raport ustaleń po teście penetracyjnym. Podczas testu przestrzegałeś specyfikacji EC-Council dotyczących certyfikacji Certified Ethical Hacker (CEH). Gdzie te informacje powinny znaleźć się w twoim raporcie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

26. Przygotowujesz dla klienta test penetracyjny z czarną skrzynką. Celem jest sprawdzenie, czy można uzyskać dostęp do poufnych danych finansowych przechowywanych na wewnętrznym serwerze bazy danych. Co klient powinien zrobić przed rozpoczęciem testu?

A. Utwórz wewnętrzne konta użytkowników dla testerów, które mają ten sam poziom uprawnień, co typowy pracownik.

B. Umieść konta użytkowników testerów na białej liście w zaporze aplikacji internetowej (WAF).

C. Skonfiguruj przypinanie certyfikatów.

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

E. Żadne z powyższych.

27. Przygotowujesz test penetracyjny białej skrzynki dla klienta. Klient wdrożył kontrolę dostępu do sieci (NAC) za pomocą protokołu IPSec, aby uniemożliwić urządzeniom niezgodnym z zasadami firmy łączenie się z bezpieczną siecią wewnętrzną. Ponieważ przeprowadzasz test białej skrzynki, systemy

testerów muszą ominąć NAC i uzyskać bezpośredni dostęp do wewnętrznej bezpiecznej sieci. Co powinien zrobić klient, aby to osiągnąć?

A. Skonfiguruj przypinanie certyfikatów.

B. Podłącz ich komputery do portu przełącznika znajdującego się w bezpiecznej sieci wewnętrznej.

C. Skonfiguruj wyjątek NAC dla każdego systemu.

D. Tymczasowo wyłącz NAC.

28. Podczas testu penetracyjnego pracownik pozostawił niemonitorowane boczne drzwi, które następnie wykorzystał tester, aby uzyskać fizyczny dostęp do obiektu klienta. Aby to się nie powtórzyło, klient całkowicie usuwa drzwi i ich ościeżnicę z budynku i wypełnia przestrzeń betonem. Jaki rodzaj reakcji na ryzyko opisano w tym scenariuszu?

A. Unikanie

B. Przeniesienie

C. Łagodzenie

D. Akceptacja

29. Podczas testu penetracyjnego pracownik pozostawił niemonitorowane boczne drzwi, które następnie wykorzystał tester, aby uzyskać fizyczny dostęp do obiektu klienta. Aby to się nie powtórzyło, klientka umieszcza na korytarzu ochroniarza i instruuje ją, aby zapobiec nieautoryzowanemu dostępowi. Jaki rodzaj reakcji na ryzyko opisano w tym scenariuszu?

A. Unikanie

B. Przeniesienie

C. Łagodzenie

D. Akceptacja

30. Twój klient prowadzi dużą witrynę e-commerce, która sprzedaje odzież i akcesoria. Podczas testu penetracyjnego tester był w stanie przechwycić numery kart kredytowych klientów podczas ich przetwarzania przez wewnętrzną aplikację do przetwarzania kart. Aby to się nie powtórzyło, klient postanawia zlecić przetwarzanie kart kredytowych zewnętrznemu procesorowi. Wszystkie transakcje są przekierowywane do zewnętrznego procesora, dzięki czemu klient nigdy nie widzi rzeczywistych danych karty kredytowej. Jaki rodzaj reakcji na ryzyko opisano w tym scenariuszu?

A. Unikanie

B. Przeniesienie

C. Łagodzenie

D. Akceptacja

31. Jaki typ skanowania luk w zabezpieczeniach najlepiej oddaje perspektywę, jaką miałby administrator systemu wewnętrznego na sieć?

A. Uwierzytelniony

B. Nieuwierzytelnione

C. Odkrycie

D. Ukrycie

32. Jaki typ skanowania podatności najlepiej oddaje perspektywę, jaką miałby haker z zewnątrz w odniesieniu do sieci?

A. Uwierzytelniony

B. Nieuwierzytelnione

C. Pełny

D. Zgodność

33. Jaki typ skanowania podatności może zwykle zidentyfikować najwięcej podatności?

A. Uwierzytelniony

B. Nieuwierzytelnione

C. Odkrycie

D. Ukrycie

34. Jaki typ skanowania podatności zwykle identyfikuje najmniejszą liczbę podatności?

A. Uwierzytelniony

B. Nieuwierzytelnione

C. Pełny

D. Zgodność

35. Przykładem jakiego typu skanowania podatności jest ping sweep?

Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

36. Atak typu ARP spoofing jest klasyfikowany jako rodzaj exploita?

A. Denial of service (DoS)

B. Man-in-the-middle

C. Distributed denial of service (DDoS)

D. VLAN hopping

37. Podczas testu penetracyjnego wykorzystującego czarną skrzynkę tester parkuje na parkingu organizacji docelowej i za pomocą laptopa przechwytuje sygnały sieci bezprzewodowej emanujące z budynku. W ten sposób jest w stanie uchwycić proces uzgadniania używany przez autoryzowanego klienta bezprzewodowego podczas łączenia się z siecią. Później ponownie wysyła ten uścisk dłoni w

sieci bezprzewodowej, umożliwiając swojemu laptopowi połączenie się z siecią bezprzewodową jako autoryzowany klient. Co to za exploit?

A. DNS cache poisoning

B. ARP spoofing

C. Pass the hash

D. Replay attack

38. Atak typu replay jest powszechnie klasyfikowany jako rodzaj exploita?

A. Denial of service (DoS)

B. NAC bypass

C. Distributed denial of service (DDoS)

D. Man-in-the-middle

39. Podczas testu penetracyjnego szarej skrzynki tester jest w stanie przechwycić pakiety przesyłane od klienta do serwera. Stacja robocza testera stanowi dla klienta serwer. Tester ma możliwość modyfikacji danych w pakietach, a następnie przesłania ich na serwer. Stacja robocza testera podszywa się pod klienta serwera. Co to za exploit?

A. Relay attack

B. DNS cache spoofing

C. Pass the hash

D. Replay attack

40. Podczas testu penetracyjnego szarej skrzynki tester jest w stanie przechwycić pakiety przesyłane od klienta do serwera. Stacja robocza testera stanowi dla klienta serwer. Tester przegląda dane w pakietach, ale nie modyfikuje ich przed przesłaniem danych na serwer. Co to za exploit?

A. Relay attack

B. DNS cache spoofing

C. Pass the hash

D. Replay attack

41. Rozważ następujący obraz:

```
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
toor             (root)
1g 0:00:00:00 DONE 1/3 (2018-11-30 03:30) 100.0g/s 12800p/s 12800c/s 12800C/s root..Root)
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

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

A. John the Ripper

B. Hydra

C. theHarvester

D. Dirbuster

42. Rozważ następujący obraz:

```
Domain Name: TESTOUT.COM
Registry Domain ID: 2178588_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-02-03T16:29:56Z
Creation Date: 1998-02-26T05:00:00Z
Registry Expiry Date: 2021-02-25T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-56.AWSDNS-07.COM
Name Server: NS-697.AWSDNS-23.NET
Name Server: NS1-07.AZURE-DNS.COM
Name Server: NS2-07.AZURE-DNS.NET
DNSSEC: unsigned
```

Które narzędzie OSINT zostało użyte do wygenerowania tego wyniku?

A. whois

B. Foca

C. Maltego

D. Censys

43. W ramach testu penetracyjnego czarnej skrzynki odkryłeś, że sygnał sieci bezprzewodowej docelowej organizacji emanuje na parking i po drugiej stronie ulicy. Chcesz uzyskać dostęp do sieci wewnętrznej za pomocą sygnału radiowego sieci bezprzewodowej. Jednak sieć bezprzewodowa jest szyfrowana. Jakich narzędzi do kompromisu bezprzewodowego możesz w tym celu użyć? (Wybierz dwa.)

A. searchsploit

B. netcat

C. OWASP ZAP

D. WiFite

E. Kismet

44. Podczas testu penetracyjnego szarej skrzynki tester musi nawiązać połączenie proxy między serwerem aplikacji sieciowej organizacji docelowej a systemami klienckimi z przeglądarkami internetowymi. Z jakich narzędzi do testowania penetracji serwera proxy sieci Web może skorzystać tester? (Wybierz dwa.)

A. searchsploit

B. Burp Suite

C. OWASP ZAP

D. Impacket

E. Empire

45. Podczas testu penetracyjnego szarej skrzynki tester chce mieć możliwość skonfigurowania exploita odwróconej powłoki, w którym skompromitowany system w sieci docelowej „dzwoni do domu” do słuchacza skonfigurowanego na laptopie testera, aby umożliwić testerowi zdalne sterowanie skompromitowany system. Jakiego narzędzia zdalnego dostępu można do tego użyć?

A. netcat

B. Responder

C. Impacket

D. BeEF

46. Jeśli chodzi o uwierzytelnianie wieloskładnikowe, które z poniższych jest przykładem czegoś, czym jesteś?

A. Hasło

B. Pytania-odpowiedź na wyzwanie

C. Skanowanie siatkówki

D. Połączenie przewodowe z wewnętrzną siecią LAN organizacji

47. Jeśli chodzi o uwierzytelnianie wieloskładnikowe, które z poniższych jest przykładem miejsca, w którym się znajdujesz?

A. Generator tokenów bezpieczeństwa

B. Hasło

C. Połączenie przewodowe z wewnętrzną siecią LAN organizacji

D. Odcisk głosu

48. Jeśli chodzi o uwierzytelnianie wieloskładnikowe, który z poniższych przykładów jest przykładem miejsca, w którym się znajdujesz?

A. Czytnik zbliżeniowy RFID

B. Generator tokenów USB

C. Odłączony generator tokenów

D. Hasło

49. Który z poniższych przykładów jest przykładem uwierzytelniania wieloskładnikowego?

A. Nazwa użytkownika + PIN

B. Czytnik zbliżeniowy RFID + połączenie sprzętowe z siecią LAN

C. Skan biometryczny + PIN

D. Hasło + pytanie wyzwanie/odpowiedź

50. Które z poniższych jest przykładem uwierzytelniania wieloskładnikowego?

A. Nazwa użytkownika + hasło

B. hasło + generator tokenów bezpieczeństwa

C. Generator tokenów USB + odłączony generator tokenów

D. Hasło + PIN

51. Zespół testerów przeprowadza ocenę organizacji. Zespół nie zajmuje się oceną szerokiego zakresu podatności. Zamiast tego przeprowadzają skoordynowany atak, którego cele są bardzo wąskie. Zasady zaangażowania określają, że mogą wykorzystywać fizyczne, elektroniczne i społeczne exploity, aby osiągnąć swój cel. Jaki rodzaj testu penetracyjnego ma miejsce w tym scenariuszu?

A. Test penetracyjny oparty na zgodności

B. Test penetracji białej skrzynki

C. Test penetracji szarej skrzynki

D. Test penetracji czarnej skrzynki

E. Test penetracyjny drużyny czerwonej

52. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta. Klient wynajmuje powierzchnię biurową w budynku dzielonym z innymi najemcami. Siedzisz w swoim samochodzie na parkingu przed biurami klientów skanując w poszukiwaniu sygnałów sieci bezprzewodowej emanujących z budynku. Zidentyfikowałeś pięć oddzielnych identyfikatorów SSID. Nie wiesz, który z nich należy do Twojego klienta, więc decydujesz się potajemnie połączyć z nimi wszystkimi, a następnie uruchomić kilka prostych skanów, aby wyizolować, która z nich jest siecią bezprzewodową Twojego klienta. Co zrobiłeś niepoprawnie w tym scenariuszu?

A. Siedzenie w samochodzie przed biurem klienta prawdopodobnie wzbudzi podejrzenia.

B. W tym scenariuszu bardziej skuteczny byłby test szarej skrzynki.

C. Sygnały bezprzewodowe emanujące na zewnątrz budynku są zwykle zbyt słabe, aby można je było wykorzystać.

D. Atakujesz sieci bezprzewodowe, które są poza zasięgiem.

53. Którzy z poniższych cyberprzestępców zazwyczaj dysponują zasobami finansowymi i wiedzą techniczną wymaganą do opracowania własnych rozległych exploitów? (Wybierz dwa.)

A. Przestępczość zorganizowana

B. Złośliwy insider

C. Scenariusz

D. Aktor państwa narodowego

E. Haktywista

54. Który z poniższych podmiotów atakujących wykorzystuje zaufanie, które zostało im zgodnie z prawem udzielone przez organizację, do złamania zabezpieczeń informacji lub systemów tej organizacji?

A. Przestępczość zorganizowana

B. Złośliwy insider

C. Scenariusz

D. Aktor państwa narodowego

E. Haktywista

55. Który z poniższych podmiotów atakujących zagrożenia zazwyczaj nie ma specjalistycznej wiedzy technicznej, aby opracować własne exploity i musi polegać na wstępnie napisanym kodzie pobranym z Internetu?

A. Przestępczość zorganizowana

B. Haktywista

C. Scenariusz

D. Aktor państwa narodowego

56. Priorytetujesz luki wykryte podczas skanowania luk. Jedna znaleziona przez Ciebie luka ma wynik w systemie Common Vulnerability Scoring System (CVSS) równy 10. Do jakiej kategorii ryzyka należy ta luka?

A. Niski

B. Średni

C. Wysoki

D. Krytyczne

57. Priorytetujesz luki wykryte podczas skanowania luk. Jedna znaleziona przez Ciebie podatność ma wynik 5.3 w Common Vulnerability Scoring System (CVSS). Do jakiej kategorii ryzyka należy ta podatność?

A. Niski

B. Średni

C. Wysoki

D. Krytyczne

58. Priorytetujesz luki wykryte podczas skanowania luk. Jedna znaleziona przez Ciebie podatność ma wynik CVSS (Common Vulnerability Scoring System) wynoszący 7,2. Do jakiej kategorii ryzyka należy ta podatność?

A. Niski

B. Średni

C. Wysoki

D. Krytyczne

59. Oceniasz wyniki skanowania podatności i zauważyłeś wspólny motyw. Odkryłeś, że prawie we wszystkich systemach Windows Server 2012 R2 organizacji docelowej brakuje tych samych krytycznych aktualizacji zabezpieczeń. Co powinieneś zrobić? (Wybierz dwa.)

A. Zatrzymaj test penetracyjny i natychmiast poinformuj klienta.

B. Zbadaj, czy stwarza to jakiekolwiek luki, które mógłbyś wykorzystać.

C. Udokumentuj wspólny motyw brakujących aktualizacji w końcowym raporcie z testu penetracyjnego.

D. Zainstaluj brakujące aktualizacje na serwerach.

E. Dokumentuj brakujące aktualizacje na swoim blogu z najlepszymi praktykami dotyczącymi testów penetracyjnych.

60. Oceniasz wyniki skanowania podatności i dokonałeś obserwacji. Odkryłeś, że organizacja ma wdrożonych wiele serwerów Linux, które nadal działają w dystrybucji wydanej w 2008 roku. Co powinieneś zrobić?

A. Mapuj luki obecne w starszych serwerach Linux na możliwe exploity.

B. Zatrzymaj test penetracyjny i natychmiast poinformuj klienta.

C. Zalecenie klientowi uaktualnienia serwerów w wiadomości e-mail.

D. Zaktualizuj serwery dla swojego klienta.

61. Jakiego programu możesz używać jako standardowy użytkownik w systemie Linux do uruchamiania programów jako root?

A. sudo

B. ps

C. top

D. nice

62. Który exploit Linuksa powoduje zastąpienie adresu zwrotnego podprogramu adresem podprogramu, który jest już obecny w pamięci procesu?

A. SGID

B. Sticky bit

C. Ret2libc

D. Unsecure sudo

63. Które z poniższych odnosi się do nazwy atrybutu, który przechowuje hasła w elemencie preferencji zasad grupy systemu Windows?

A. cPassword

B. TGT

C. TGS

D. LSASS

64. Podczas testu penetracyjnego odkrywasz, że administrator używa protokołu LDAP w postaci zwykłego tekstu na porcie 388 do aktualizacji kont użytkowników w swojej usłudze katalogowej zgodnej z LDAP, w tym poświadczeń użytkowników. Co powinieneś polecić klientowi, aby to naprawić?

A. Zalecamy zaprzestanie używania klientów LDAP do zarządzania kontami użytkowników.

B. Zalecamy korzystanie z protokołu SSL z obsługą protokołu SSL na porcie 636.

C. Zalecamy, aby przeszli na usługę katalogową inną niż LDAP.

D. Zalecamy używanie protokołu LDAP z obsługą SSH na porcie 22.

65. Podczas testu penetracyjnego szarej skrzynki tester loguje się do domeny organizacji docelowej i żąda nazwy zasady usługi (SPN) dla zarejestrowanej usługi. Otrzymano zgłoszenie, a tester przełącza go w tryb offline i próbuje złamać jego szyfrowanie. Jak nazywa się ten exploit?

A. Sandbox escape

B. Kerberoasting

C. DLL hijacking

D. Cold boot attack

66. Która struktura kontroli jest uważana za strukturę kontroli przepływu?

A. pętla while

B. pętla for

C. pętla until

D. if/then/else

67. Która struktura kontrolna będzie przetwarzać w kółko tak długo, jak określony warunek będzie miał wartość false?

A. pętla while

B. pętla for

C. pętla until

D. if/then/else

68. Która struktura kontroli będzie przetwarzać określoną liczbę razy?

A. pętla while

B. pętla for

C. pętla until

D. if/then/else

E. case

69. Musisz utworzyć skrypt PowerShell, który poprosi użytkownika o wprowadzenie wartości. Które polecenie zaakceptuje wartość wprowadzoną przez użytkownika i przypisze ją do zmiennej o nazwie TargetHost?

A. TargetHost = input('Please enter a hostname:')

B. read TargetHost

C. TargetHost = gets

D. $TargetHost = read-host -Prompt

70. Które polecenie w skrypcie PowerShell spowoduje zapisanie na ekranie wartości zmiennej o nazwie TargetHost?

A. echo $TargetHost

B. print (TargetHost)

C. writeln TargetHost

D. puts TargetHost

71. Po zakończeniu testowania dla klienta, tester ustala priorytety wyników i zaleceń w podsumowaniu wykonawczym. Która z poniższych kwestii byłaby najbardziej korzystna dla klienta?

A. Dostępność łatek i innych środków zaradczych

B. Poziomy trudności wykorzystania zidentyfikowanych podatności

C. Tolerancja ryzyka organizacji klienta

D. Czas potrzebny na wykonanie każdego kroku

72. Młodszy technik w dziale IT organizacji przeprowadza test penetracyjny w korporacyjnej aplikacji internetowej. Podczas testowania technik odkrywa, że aplikacja może ujawnić tabelę SQL zawierającą wszystkie informacje o koncie użytkownika i hasłach. Jak technik powinien powiadomić kierownictwo?

A. Technik powinien połączyć się z serwerem SQL przy użyciu tych informacji i zmienić hasła kilku kont niekrytycznych, aby zademonstrować kierownictwu weryfikację koncepcji.

B. Technik powinien udokumentować wyniki za pomocą podsumowania wykonawczego, w tym zaleceń i zrzutów ekranu, które należy przekazać kierownictwu.

C. Technik powinien powiadomić zespół programistów o odkryciu i zasugerować wymuszenie sprawdzania poprawności danych wejściowych w ciągach zapytań SQL aplikacji internetowej.

D. Technik powinien poprosić kierownictwo o utworzenie zapytania ofertowego (RFP), aby rozpocząć formalną współpracę z profesjonalną firmą zajmującą się testami penetracyjnymi.

73. Jesteś analitykiem bezpieczeństwa i przeglądasz wyniki ostatniego wewnętrznego skanowania luk w zabezpieczeniach, które zostało przeprowadzone w odniesieniu do usług intranetowych. Raporty ze skanowania wskazywały na krytyczną lukę w zabezpieczeniach. W raporcie wskazano, co następuje:

Tytuł: Luka umożliwiająca zdalne wykonanie polecenia na serwerze WWW

Ocena: krytyczna (CVSS 10.0)

Aktor zagrożenia: dowolny zdalny użytkownik serwera WWW

Zaufanie: pewne

Zalecenie: zastosuj poprawki dostawcy

Co powinieneś zrobić najpierw?

A. Zastosuj ocenę ryzyka i jej wpływ na organizację.

B. Wykorzystaj serwer, aby ustalić, czy skanowanie wykazało fałszywy alarm.

C. Poinformuj kierownictwo wyższego szczebla o luce.

D. Zorganizuj krytyczne poprawki poza cyklem.

74. Jesteś testerem penetracyjnym i podczas czyszczenia po teście penetracyjnym okazuje się, że klient nie ma niezbędnych narzędzi do usuwania danych. Potrzebne narzędzia zostały następnie przekazane technikom, którzy ich potrzebowali. Na jakim etapie powinieneś ponownie przyjrzeć się temu problemowi?

A. Podczas wyciągniętych lekcji

B. Podczas łagodzenia

C. W trakcie przygotowania

D. Podczas raportowania

75. Omawiasz uwierzytelnianie wieloskładnikowe z klientem. Klient prosi o przykład, czym jest uwierzytelnianie wieloskładnikowe. Co powiesz klientowi, co spełni wymagania uwierzytelniania wieloskładnikowego?

A. Korzystanie z biometrycznych odcisków palców i rozpoznawania głosu

B. Korzystanie z kart inteligentnych i kodów PIN

C. Korzystanie ze skanów siatkówki i rozpoznawania głosu

D. Używanie nazw użytkowników, kodów PIN i numerów identyfikacyjnych pracowników

76. IEEE definiuje trzy ramki bezprzewodowe w ramach standardu bezprzewodowego dla urządzeń sieciowych Wi-Fi. Która ramka jest ostatecznie używana do uwierzytelniania?

A. Ramka zarządzania

B. Ramka kontrolna

C. Ramka monitora

D. Ramka danych

77. W sieciach bezprzewodowych, która ramka jest rodzajem ramki zarządzania, która identyfikuje identyfikator SSID, typ szyfrowania i adres MAC punktu dostępowego?

A. Ramka sygnalizacyjna

B. Ramka żądania sondy

C. Ramka danych

D. Ramka odpowiedzi stowarzyszenia

78. Systemy operacyjne czasu rzeczywistego (RTOS) zazwyczaj znajdują się w urządzeniach wbudowanych, takich jak routery, kamery IP, urządzenia medyczne i tak dalej. Istnieje wiele klasyfikacji urządzeń RTOS. Która klasyfikacja musi być zgodna z ograniczeniami czasowymi dla powiązanego zadania?

A. Hard

B. Firm

C. Soft

D. Wszystkie powyższe

79. Burp Suite Pro to internetowe narzędzie do oceny bezpieczeństwa, które zapewnia możliwość proxy i obsługi żądań testów ręcznych podczas testu penetracyjnego. Jak nazywa się podobne narzędzie, opracowane przez OWASP, które zapewnia podobne możliwości testowania aplikacji internetowych?

A. ZAP

B. DirBuster

C. Webkoza

D. Nessusa

80. Podczas pentestu odkrywasz plik sitemap.xml i plik crossdomain.xml. Pliki te mogą dostarczyć przydatnych informacji do mapowania katalogów internetowych i plików, które w innym przypadku musiałyby być wymuszane metodą brute-force. Jak nazywa się inny plik, który może udostępniać adresy URL i lokalizacje URI, które uniemożliwiają wyszukiwarkom indeksowanie określonych lokalizacji?

A. policy.xml

B. site.txt

C. robots.txt

D. crossdomain.policy