1. Który rodzaj testu penetracyjnego najlepiej odwzorowuje perspektywę napastnika w świecie rzeczywistym?

A. Ocena szarej skrzynki

B. Ocena czarnej skrzynki

C. Ocena obiektywna

D. Ocena białej skrzynki

2. Konsultant został zatrudniony przez organizację do przeprowadzenia testu penetracyjnego. Celem testu jest aplikacja bazy danych HR organizacji. Tester otrzymał biurko, komputer podłączony do sieci organizacji oraz schemat sieci. Jednak tester nie otrzymał żadnych danych uwierzytelniających. Jaki rodzaj testu jest przeprowadzany w tym scenariuszu?

A. Ocena oparta na zgodności

B. Ocena czarnej skrzynki

C. Ocena szarej skrzynki

D. Ocena białej skrzynki

3. Konsultant został zatrudniony przez organizację do wykonania testu penetracyjnego. Celem testu jest strona e-commerce organizacji. Tester, zlokalizowany w innym mieście, użyje kilku różnych narzędzi do testowania penetracji, aby przeanalizować witrynę i zaatakować ją. Tester nie ma żadnych informacji o witrynie ani żadnych danych uwierzytelniających. Jaki rodzaj testu jest przeprowadzany w tym scenariuszu?

A. Ocena białej skrzynki

B. Ocena czarnej skrzynki

C. Ocena obiektywna

D. Ocena szarej skrzynki

4. Konsultant został zatrudniony przez organizację do przeprowadzenia testu penetracyjnego. Celem testu są wewnętrzne zapory ogniowe organizacji. Tester otrzymał biurko, komputer podłączony do sieci organizacji oraz schemat sieci. Tester otrzymał również dane uwierzytelniające z dość wysokim poziomem dostępu. Jaki rodzaj testu jest przeprowadzany w tym scenariuszu?

A. Ocena szarej skrzynki

B. Ocena czarnej skrzynki

C. Ocena oparta na celach

D. Ocena białej skrzynki

5. Który rodzaj testu penetracyjnego najlepiej skupia czas i wysiłki testera, jednocześnie zapewniając przybliżony obraz tego, co zobaczy prawdziwy atakujący?

A. Ocena szarej skrzynki

B. Ocena czarnej skrzynki

C. Ocena oparta na celach

D. Ocena białej skrzynki

6. Przeprowadzasz test penetracyjny „czarnej skrzynki” dla dużej organizacji zajmującej się hurtową sprzedażą importowanych urządzeń elektronicznych w Stanach Zjednoczonych. Musisz zbadać adres IP serwera internetowego organizacji, aby zobaczyć, jakie informacje są z nim powiązane, takie jak wersja protokołu SSL lub TLS oraz używany przez niego zestaw szyfrów. Którego narzędzia z zestawu narzędzi do testowania penetracji możesz użyć, aby to zrobić?

A. Censys

B. nslookup

C. Maltego

D. Shodan

7. Przeprowadzasz test penetracyjny z czarną skrzynką dla dużej organizacji finansowej. Chcesz przeszukać Internet w poszukiwaniu dokumentów powiązanych z organizacją (takich jak dokumenty Microsoft Word lub PowerPoint) i przeanalizować metadane każdego pliku w celu uzyskania przydatnych informacji. Którego narzędzia z zestawu narzędzi do testowania penetracji możesz użyć, aby to zrobić?

A. Censys

B. Shodan

C. nmap

D. Organizacje wykorzystujące odciski palców ze zbiorami archiwalnymi (FOCA)

8. Konsultant został zatrudniony przez organizację w celu przeprowadzenia testu penetracyjnego czarnej skrzynki. Wie, że urządzenia Internetu rzeczy (IoT) często wykorzystują słabe mechanizmy bezpieczeństwa, które może wykorzystać tester penetracji. Chce sprawdzić, czy w organizacji docelowej wdrożono którekolwiek z tych urządzeń. Jakiego narzędzia mogłaby użyć do tego?

A. Censys

B. Shodan

C. theHarvester

D. Maltego

9. Konsultant został zatrudniony przez organizację w celu przeprowadzenia testu penetracyjnego czarnej skrzynki. Korzystała z różnych narzędzi, aby zebrać OSINT o docelowych informacjach. Jej wysiłki były bardzo udane. W rzeczywistości zebrała tak wiele informacji, że ma trudności z uporządkowaniem ich w format, z którego będzie mogła efektywnie korzystać. Jakiego narzędzia mogłaby użyć do uporządkowania zebranych informacji?

A. Censys

B. Shodan

C. theHarvester

D. Maltego

10. Konsultant został zatrudniony przez organizację w celu przeprowadzenia testu penetracyjnego czarnej skrzynki. Chce przeprowadzić szczegółowe skanowanie publicznego serwera internetowego organizacji docelowej, aby zobaczyć, czego może się dowiedzieć. Jakiego narzędzia powinna użyć, aby to osiągnąć?

A. nmap

B. Shodan

C. whois

D. Maltego

11. Która technika socjotechniki polega na przesłuchiwaniu pracownika przy użyciu zastraszania w celu zebrania informacj
i?

A. Phishing

B. Smishing

C. Podszywanie się

D. Przesłuchanie

12. Przeprowadzasz test penetracyjny „czarnej skrzynki” dla dużej organizacji finansowej. Korzystając z technik rozpoznawczych, zidentyfikowałeś dostawcę obsługującego automaty w głównej siedzibie organizacji. Ubierasz się w podobny mundur jak pracownicy sprzedawcy. Kupujesz również wózek ręczny i kilka skrzynek napoju gazowanego. Recepcjonistka organizacji docelowej umożliwia wejście i kieruje do pokoju socjalnego. Jakiego rodzaju exploita użyłeś w tym scenariuszu?

A. Podszywanie się

B. Smishing

C. Vishing

D. Pozyskiwanie

13. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji produkcyjnej. Korzystając z technik rozpoznawczych, zidentyfikowałeś dostawcę, który obsługuje drukarki w centrali organizacji. Ubierasz się w podobny mundur jak pracownicy tego sprzedawcy. Kupujesz również zestaw narzędzi zawierający narzędzia powszechnie używane przez techników zajmujących się naprawą drukarek. Recepcjonistka organizacji docelowej umożliwia wejście i kieruje do kłopotliwej drukarki. Podczas „pracy” na tej drukarce rozmawiasz z pobliskimi pracownikami, aby zebrać informacje. Jakich exploitów użyłeś w tym scenariuszu? (Wybierz dwa.)

A. Podszywanie się

B. Whling

C. Phishing

D. Przesłuchanie

E. Pozyskiwanie

14. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji produkcyjnej. Korzystając z technik rozpoznawczych, zidentyfikowałeś dostawcę, który obsługuje drukarki w centrali organizacji. Ubierasz się w podobny mundur jak pracownicy tego sprzedawcy. Kupujesz również zestaw narzędzi zawierający narzędzia powszechnie używane przez techników zajmujących się naprawą drukarek. Recepcjonistka organizacji docelowej umożliwia wejście i kieruje do kłopotliwej drukarki. Podczas „pracy" w organizacji dyskretnie obserwujesz pracowników podczas pisania, próbując zebrać poufne informacje. Jakich exploitów użyłeś w tym scenariuszu? (Wybierz dwa.)

A. Surfowanie na ramieniu

B. Phishing

C. Podszywanie się

D. Przesłuchanie

E. Pozyskiwanie

15. Przeprowadzasz test penetracyjny czarnej skrzynki dla średniej wielkości organizacji produkcyjnej. Korzystając z technik rozpoznania i phishingu, złamałeś hasło do konta e-mail pracownika. Używasz tego konta do przesłuchiwania innych pracowników w celu zebrania poufnych informacji i dokumentów. Jakich exploitów użyłeś w tym scenariuszu? (Wybierz dwa.)

A. Surfowanie na ramieniu

B. Phishing

C. Podszywanie się

D. Przesłuchanie

E. Pozyskiwanie

16. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Zidentyfikowano hosta wewnętrznego o adresie IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie połączenia TCP tego hosta. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.1 –sL

B. nmap 192.168.1.1 –T1

C. nmap 192.168.1.1 -sT

D. nmap 192.168.1.1 -f

17. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Zidentyfikowano hosta wewnętrznego o adresie IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie portu UDP tego hosta. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.1 –sL

B. nmap 192.168.1.1 –U

C. nmap 192.168.1.1 -sT

D. nmap 192.168.1.1 -sU

18. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Musisz użyć narzędzia nmap na swoim laptopie, aby wykryć wszystkie hosty w podsieci 192.168.1.0 (która używa maski podsieci 255.255.255.0) bez faktycznego skanowania tych hostów. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.0/24 –sL

B. nmap 192.168.1.0/24 --lista

C. nmap 192.168.1.1-254 -sW

D. nmap 192.168.1.1-254 -sM

19. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Zidentyfikowano hosta wewnętrznego o adresie IP 192.168.1.1 jako potencjalny cel. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie TCP ACK tego hosta. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.1 –sA

B. nmap 192.168.1.1 –T1

C. nmap 192.168.1.1 -sT

D. nmap 192.168.1.1 -ACK

20. Przeprowadzasz test penetracyjny białej skrzynki dla klienta. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie każdego hosta w podsieci 192.168.1.0 (która używa maski podsieci 255.255.255.0), ale bez skanowania hosta o adresie IP 192.168.1.250 (który podejrzewasz, że jest hostem honeypot). Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.1-254

B. nmap 192.168.1.0/24 --noscan 192.168.1.250

C. nmap 192.168.1.0/24 --wyklucz 192.168.1.250

D. nmap 192.168.1.1-254 --pomiń 192.168.1.250

//

21. Twoja organizacja przeprowadza dla klienta test penetracyjny „czarnej skrzynki”. W Twoim zespole ds. testów penetracyjnych jest pięciu członków. Podczas testu stale komunikujesz się z innymi członkami zespołu za pośrednictwem poczty elektronicznej i wiadomości tekstowych, aby upewnić się, że wszyscy wiedzą, co robią inni. Jak nazywa się ten proces?

A. Świadomość sytuacyjna

B. Metryki i miary

C. Dekonflikt

D. Normalizacja danych

22. Twoja organizacja przeprowadza dla klienta test penetracyjny z wykorzystaniem czarnej skrzynki. W Twoim zespole ds. testów penetracyjnych jest pięciu członków. Podczas testu stale komunikujesz się z innymi członkami zespołu za pośrednictwem poczty e-mail i wiadomości tekstowych, aby koordynować harmonogram działań, w tym rekonesans, wyliczanie, exploity i tak dalej. Jak nazywa się ten proces?

A. Świadomość sytuacyjna

B. Deeskalacja

C. Dekonflikt

D. Normalizacja danych

23. Podczas testu penetracyjnego organizacja klienta zaczyna otrzymywać skargi od pracowników zdalnych wskazujące, że sieć VPN organizacji nie działa. Administrator sieci wykrywa trwający atak odmowy sieci lokalnej (LAND), którego celem jest serwer VPN firmy na obrzeżach sieci. Pracownicy zdalni nie są w stanie pracować, więc administrator dzwoni do testera penetracji i prosi o wycofanie ataku. Jak nazywa się ta ścieżka komunikacji?

A. Świadomość sytuacyjna

B. Deeskalacja

C. Dekonflikt

D. Zmiana priorytetów celów

24. Podczas testu penetracyjnego administrator sieci organizacji klienckiej wykrywa trwający atak typu teardrop, którego celem jest router obwodowy firmy. Administrator dzwoni do testera penetracji, aby sprawdzić, czy atak jest częścią testu penetracyjnego. Jak nazywa się ta ścieżka komunikacji?

A. Świadomość sytuacyjna

B. Metryki i miary

C. Dekonflikt

D. Normalizacja danych

25. Twoja organizacja przeprowadza dla klienta test penetracyjny z wykorzystaniem czarnej skrzynki. W Twoim zespole jest trzech testerów. Na początku procesu masz spotkanie zespołu, aby zaplanować, jak test zostanie przeprowadzony, kiedy nastąpią określone czynności i którzy członkowie zespołu będą odpowiedzialni za wykonanie określonych zadań. Jak nazywa się ten proces?

A. Konflikt

B. Deeskalacja

C. Świadomość sytuacyjna

D. Zmiana priorytetów celów

26. Przeprowadzasz test penetracyjny dla klienta. Oryginalny test wymaga przetestowania bezpieczeństwa jednego ze zdalnych oddziałów klienta. Klient zadzwonił dzisiaj i poinformował, że jest zaniepokojony gotowością drugiego oddziału w zakresie bezpieczeństwa. Nalegali, aby rozszerzyć test penetracyjny o tę drugą witrynę. Jaki proces wystąpił w tym scenariuszu?

A. Należyta staranność

B. Akceptacja ryzyka

C. Modelowanie zagrożeń

D. Pełzanie zakresu

27. Klient poprosił Cię o przeprowadzenie testu penetracyjnego białej skrzynki. Jej organizacja ma biura w Wielkiej Brytanii, Arabii Saudyjskiej, Pakistanie i Hongkongu. Ładujesz zestaw narzędzi do testów penetracyjnych na laptopie i udajesz się do każdego biura, aby przeprowadzić ocenę na miejscu. Co zrobiłeś niepoprawnie w tym scenariuszu?

A. Transport za granicę niektórych programów i sprzętu do testów penetracyjnych może być nielegalny.

B. Laptop nie ma wystarczającej mocy obliczeniowej, aby skutecznie przeprowadzić test penetracyjny.

C. Koszty podróży można zmniejszyć, przeprowadzając ocenę zdalnie z miejsca zamieszkania testera.

D. Nic. Zrobiłeś wszystko poprawnie.

28. Klient poprosił Cię o przeprowadzenie testu penetracyjnego białej skrzynki. Jej organizacja ma biura w Stanach Zjednoczonych, Indonezji, Tajlandii i Singapurze. Aby uniknąć międzynarodowego transportu oprogramowania do testowania penetracji, przesyłasz je na swoje konto Dysku Google. Następnie udajesz się do każdej witryny, pobierasz oprogramowanie i uruchamiasz je lokalnie na swoim laptopie. Czy w tym scenariuszu odpowiednio obsłużyłeś oprogramowanie do testów penetracyjnych?

A. Tak, korzystanie z Dysku Google w celu uzyskania dostępu do oprogramowania na całym świecie chroni przed ściganiem.

B. Nie, większość obcych krajów blokuje dostęp do Dysku Google.

C. Nie, transport większości oprogramowania do testów penetracyjnych do tych krajów jest legalny.

D. Nie, międzynarodowe przesyłanie większości oprogramowania do testów penetracyjnych za pośrednictwem Internetu jest nielegalne.

29. Jesteś proszony o wykonanie testu penetracyjnego dla organizacji, której biura znajdują się w Nowym Jorku, Los Angeles i Fargo. Które przepisy i regulacje dotyczące bezpieczeństwa cybernetycznego musisz sprawdzić, kiedy przeprowadzasz ocenę?

A. Amerykańskie federalne prawo dotyczące cyberbezpieczeństwa

B. Stanowe przepisy dotyczące cyberbezpieczeństwa w Nowym Jorku, Kalifornii i Północnej Dakocie

C. Lokalne przepisy dotyczące cyberbezpieczeństwa w każdej fizycznej lokalizacji

D. Regulamin Interpolu

30. Klient poprosił Cię o przeprowadzenie testu penetracyjnego białej skrzynki. Celem jest ocena bezpieczeństwa ich aplikacji internetowych. Aplikacje te wykorzystują protokół SOAP (Simple Object Access Protocol). Podczas procesu określania zakresu stwierdzasz, że pomocne byłoby, gdybyś miał dostęp do wewnętrznej dokumentacji organizacji dla tych aplikacji. O które z poniższych pytań powinieneś zapytać swojego klienta?

A. Dokumentacja języka opisu usług sieciowych (WSDL)

B. Dokumentacja zestawu programistycznego (SDK)

C. Dokumentacja języka opisu aplikacji internetowych (WADL)

D. Dokumentacja interfejsu programowania aplikacji (API)

31. Podczas fazy zbierania informacji testu penetracji czarnej skrzynki musisz podsłuchiwać emisje o częstotliwości radiowej pochodzące z obiektu celu i próbować przechwycić dane z jego sieci bezprzewodowej. Jesteś zaparkowany na parkingu organizacji. Chcesz użyć aircrack-ng do złamania szyfrowania używanego przez sieć Wi-Fi. Aby to osiągnąć, musisz najpierw przechwycić uzgadnianie uwierzytelniania. Jakie narzędzie należy uruchomić na laptopie, aby to zrobić?

A. airodump-ng

B. aireplay-ng

C. aircrack-ng

D. nmap

32. Podczas fazy zbierania informacji w teście penetracji czarnej skrzynki musisz podsłuchiwać emisje o częstotliwości radiowej pochodzące z obiektu celu i próbować przechwycić dane z jego sieci bezprzewodowej. Przechwyciłeś już uzgadnianie uwierzytelniania. Następnie musisz ponownie uwierzytelnić klienta bezprzewodowego, aby rozpocząć przechwytywanie danych. Jakie narzędzie należy uruchomić na laptopie, aby to zrobić?

A. airodump-ng

B. aireplay-ng

C. aircrack-ng

D. nmap

33. W ramach testu penetracji szarej skrzynki musisz przechwycić pakiety w sieci przewodowej. Jak należy skonfigurować interfejs sieci przewodowej w laptopie, aby to osiągnąć?

A. Ustaw tryb monitorowania.

B. Ustaw na tryb promiscuous.

C. Ustaw tryb przechwytywania.

D. Ustaw tryb IEEE 802.1x.

34. W ramach testu penetracji szarej skrzynki musisz przechwycić pakiety w sieci przewodowej. Skonfigurowałeś interfejs sieciowy w swoim laptopie, aby akceptował wszystkie ramki przesyłane przez medium sieciowe, i zainstalowałeś Wireshark. Jednak po uruchomieniu Wireshark widzisz tylko ramki zaadresowane specjalnie do twojego laptopa. Dlaczego się to stało?

A. Zapora sieciowa na komputerze przenośnym blokuje wszystkie inne ramki.

B. W przełączniku włączono filtrowanie adresów MAC.

C. Sieć korzysta z koncentratora.

D. Sieć korzysta z przełącznika.

35. W ramach testu penetracji szarej skrzynki musisz przechwycić pakiety w sieci przewodowej. Skonfigurowałeś interfejs sieciowy w swoim laptopie, aby akceptował wszystkie ramki przesyłane przez medium sieciowe, i zainstalowałeś Wireshark. Jednak po uruchomieniu Wireshark widzisz tylko ramki zaadresowane specjalnie do twojego laptopa. Jak możesz to naprawić?

A. Wyłącz zaporę sieciową hosta na swoim laptopie.

B. Wyłącz filtrowanie adresów MAC na przełączniku.

C. Wymień przełącznik sieciowy na koncentrator.

D. Podłącz laptopa do portu lustrzanego na przełączniku.

36. Podczas fazy zbierania informacji testu penetracji szarej skrzynki uruchamiasz polecenie NBTSTAT -c w sieci lokalnej. Jeden z wierszy na wyjściu brzmi następująco:

Name Type Host Address Life [sec]

DEV-1 <20> UNIQUE 10.0.0.3 517

Co wiesz o hoście DEV-1?

A. To jest serwer.

B. Jest to stacja robocza.

C. To jest router.

D. Jest to urządzenie bezprzewodowe.

37. Podczas fazy zbierania informacji testu penetracji szarej skrzynki uruchamiasz polecenie NBTSTAT -c w sieci lokalnej. Jeden z wierszy na wyjściu brzmi następująco:

Name Type Host Address Life [sec]

PROD-9 <00> UNIQUE 10.0.0.132 517

Co wiesz o hoście PROD-9?

A. To jest serwer.

B. Jest to stacja robocza.

C. To jest router.

D. Jest to urządzenie bezprzewodowe.

38. Które z poniższych stwierdzeń są prawdziwe w przypadku protokołu LLMNR (Link-Local Multicast Name Resolution)? (Wybierz dwa.)

A. Jest powszechnie używany w przypadku braku serwera DNS.

B. Nie jest obsługiwany przez hosty Linux.

C. Nie jest obsługiwany przez hosty Windows.

D. Jest używany tylko przez routery, a nie przez stacje robocze czy serwery.

E. Umożliwia hostowi IPv6 rozwiązywanie nazw hostów na tym samym łączu lokalnym.

39. Które z poniższych opisują zagrożenia bezpieczeństwa związane z używaniem protokołu LLMNR? (Wybierz dwa.)

A. Dane są przesyłane w postaci zwykłego tekstu.

B. Brak kontroli bezpieczeństwa.

C. Złośliwy host może reklamować się jako dowolny host, którego chce.

D. Może być użyty do ułatwienia ataku DDoS.

E. Tworzy nadmierny ruch w sieci.

40. Jakie są funkcje protokołu Server Message Block (SMB)? (Wybierz dwa.)

A. Udostępnianie plików w sieci

B. Przesyłanie wiadomości e-mail między agentami przesyłania poczty (MTA)

C. Udostępnianie drukarek w sieci

D. Mapowanie adresów IP na adresy MAC

E. Przesyłanie wiadomości e-mail do agenta użytkownika poczty (MUA)

41. Penetracja przeprowadza dla klienta test szarej skrzynki. Tester chce spróbować wygenerować „złoty bilet" protokołu Kerberos w celu złamania zabezpieczeń usług w docelowej domenie Active Directory. Jakiego narzędzia można do tego użyć?

A. Mimikatz

B. John the Ripper

C. W3AF

D. ncat

42. Które z poniższych narzędzi można zakwalifikować jako skanery luk w zabezpieczeniach? (Wybierz dwa.)

A. Nikto

B. ZESTAW

C. W3AF

D. Meduza

E. Hydra

43. Które z poniższych są powszechnie używane do przeprowadzania ataków na hasła typu brute-force? (Wybierz dwa.)

A. BeFF

B. Drozer

C. W3AF

D. Meduza

E. Hydra

44. Którego z poniższych można użyć do przeprowadzenia ataków typu brute-force z hasłami? (Wybierz dwa.)

A. Imperium

B. Patator

C. Powersplot

D. Aircrack-ng

E. Studio APK

45. Które z poniższych narzędzi do penetracji są oparte na środowisku Windows PowerShell? (Wybierz dwa.)

A. BeEF

B. SET

C. Empire

D. PowerSploit

E. Hopper

46. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu udało Ci się wykorzystać exploita phishingowego do zebrania danych uwierzytelniających od kilku pracowników. Aby wyeliminować tę lukę, zaleca się, aby klient przeprowadził obowiązkową sesję szkoleniową dotyczącą świadomości bezpieczeństwa dla wszystkich pracowników. Jakie to rozwiązanie?

A. Technologiczne

B. Ludzie

C. Proces

D. Skalowalny

47. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zauważasz, że wszystkie komputerowe systemy Windows w organizacji mają to samo hasło przypisane do lokalnego konta użytkownika Administrator. Co możesz polecić, aby rozwiązać ten problem?

A. Zaszyfruj hasła.

B. Implementuj wymagania dotyczące złożoności hasła.

C. Zaimplementuj blokadę intruza.

D. Losuj poświadczenia administratora lokalnego.

48. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zauważasz, że wszystkie komputerowe systemy Windows w organizacji mają to samo hasło przypisane do lokalnego konta użytkownika Administrator. Kiedy zgłaszasz to klientowi, wskazują, że są tego świadomi i że zrobili to celowo, aby zmniejszyć złożoność zarządzania. Jakie rozwiązanie możesz polecić, aby usunąć lukę bez zwiększania złożoności zarządzania?

A. Losuj poświadczenia administratora lokalnego.

B. Wdrożenie LAPS.

C. Uczyń wszystkich lokalnych użytkowników Windows członkami lokalnej grupy Administratorzy.

D. Uczyń wszystkich użytkowników domeny Windows członkami grupy Administratorzy domeny.

49. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zgłaszasz, że udało Ci się naruszyć konta kilku użytkowników w systemie Windows, ponieważ używali oni haseł, takich jak hasło, aaa i 1234. Które z poniższych ustawień zasad grupy domeny można im zalecić, aby zapobiec złożoności słabych haseł? (Wybierz dwa.)

A. Przechowuj hasła przy użyciu odwracalnego szyfrowania.

B. Hasło musi spełniać wymagania dotyczące złożoności.

C. Minimalna długość hasła.

D. Ustawienia weryfikacji ścieżki certyfikatu.

E. Klient usług certyfikatów – Autorejestracja.

50. Które z poniższych ustawień zasad grupy systemu Windows można wykorzystać do uniemożliwienia użytkownikowi wielokrotnego używania tego samego hasła?

A. Wymuszaj historię haseł

B. Przechowuj hasła przy użyciu odwracalnego szyfrowania

C. Minimalna długość hasła

D. Hasło musi spełniać wymagania dotyczące złożoności

51. Które z poniższych najlepiej opisuje pojęcie poufności w kontekście testów penetracyjnych?

A. Zapobieganie nieautoryzowanemu dostępowi do informacji

B. Zapobieganie nieautoryzowanym modyfikacjom informacji

C. Zapewnienie, że informacje pozostają dostępne dla autoryzowanego dostępu

D. Zapobieganie legalnemu dostępowi do informacji

52. Które z poniższych najlepiej opisuje pojęcie integralności w kontekście testów penetracyjnych?

A. Zapobieganie nieautoryzowanemu dostępowi do informacji

B. Zapobieganie nieautoryzowanym modyfikacjom informacji

C. Zapewnienie, że informacje pozostają dostępne dla autoryzowanego dostępu

D. Uzyskanie nieautoryzowanego dostępu do informacji

53. Które z poniższych najlepiej opisuje termin dostępność w kontekście testów penetracyjnych?

A. Zapobieganie nieautoryzowanemu dostępowi do informacji

B. Zapobieganie nieautoryzowanym modyfikacjom informacji

C. Zapewnienie, że informacje pozostają dostępne dla autoryzowanego dostępu

D. Dokonywanie nieautoryzowanych zmian w informacjach

54. Które z poniższych najlepiej opisuje termin „ujawnienie” w kontekście testów penetracyjnych?

A. Uzyskanie nieautoryzowanego dostępu do informacji

B. Dokonywanie nieautoryzowanych zmian w informacjach

C. Zapobieganie zgodnemu z prawem wykorzystaniu informacji

D. Publiczne potwierdzenie, że nastąpiło naruszenie bezpieczeństwa i informacje zostały naruszone

55. Które z poniższych najlepiej opisuje termin „zmiana” w kontekście testów penetracyjnych?

A. Uzyskanie nieautoryzowanego dostępu do informacji

B. Dokonywanie nieautoryzowanych zmian w informacjach

C. Zapobieganie zgodnemu z prawem wykorzystaniu informacji

D. Wykorzystywanie jednego udanego kompromisu do skompromitowania innego niedostępnego w inny sposób systemu w sieci

56. Które z poniższych jest przykładem nietradycyjnego zasobu?

A. Serwer bazy danych

B. Router

C. Monitor telewizyjny z dostępem do Internetu

D. Urządzenie filtrujące zawartość

57. Które z poniższych jest przykładem nietradycyjnego zasobu?

A. Serwer e-mail

B. Sprzęt produkcyjny sterowany komputerowo

C. Bezprzewodowy punkt dostępowy

D. Komputer stacjonarny typu „wszystko w jednym”

58. W ramach fazy zbierania informacji testu penetracyjnego czarnej skrzynki musisz wykonać transfer strefy DNS domeny organizacji docelowej. Którego z poniższych poleceń możesz w tym celu użyć? (Wybierz dwa.)

A. dig axfr @nameserver target_domain

B. host -t serwer nazw domeny_docelowej axfr

C. nslookup –type=ns domena_docelowa

D. nmap get-domain-transfer domena_docelowa

59. Przeprowadzasz test penetracji szarej skrzynki. Chcesz stworzyć niestandardowy pakiet, aby przetestować, jak serwer odpowiada i zobaczyć, jakimi informacjami odpowiada. Jakiego narzędzia możesz użyć, aby to zrobić?

A. hping

B. ping

C. nmap

D. Wireshark

60. Przeprowadzasz test penetracji czarnej skrzynki. Użyłeś theHarvester do wyliczenia dużej liczby adresów e-mail użytkowników w organizacji docelowej. Co możesz zrobić z tymi informacjami? (Wybierz dwa.)

A. Przeprowadź exploita phishingowego.

B. Wysyłaj spam.

C. Wymień wewnętrzne konta użytkowników.

D. Wykonaj transfer strefy DNS.

61. Podczas testu penetracyjnego czarnej skrzynki tester odkrywa, że bezprzewodowy punkt dostępowy organizacji został skonfigurowany przy użyciu nazwy użytkownika administratora i hasła administratora. Tester uzyskuje dostęp administracyjny do punktu dostępu. Jaki rodzaj luki w uwierzytelnianiu wystąpił w tym scenariuszu?

A. Wykorzystanie słabych danych uwierzytelniających

B. Atak przekierowania

C. Atak na domyślne dane uwierzytelniające

D. brutalne forsowanie poświadczeń

62. Administrator sieci w organizacji, która jest celem testu penetracyjnego, skonfigurował jej zaporę sieciową z administracyjną nazwą użytkownika admin i hasłem password. Na który exploit uwierzytelniania jest podatne to urządzenie?

A. Wykorzystanie słabych danych uwierzytelniających

B. Atak przekierowania

C. Przejmowanie sesji

D. Exploit Kerberos

63. Podczas testu penetracyjnego szarej skrzynki tester może uruchomić exploita, który umożliwia jej otrzymanie biletu nadania biletu (TGT) z centrum dystrybucji kluczy (KDC) w domenie Active Directory organizacji. Jaki rodzaj luki w uwierzytelnianiu wystąpił w tym scenariuszu?

A. Wykorzystanie danych uwierzytelniających do brutalnego wymuszania

B. Atak przekierowania

C. Przejmowanie sesji

D. Exploit Kerberos

64. Które exploity autoryzacji modyfikują parametr w żądaniu HTTP w celu uzyskania nieautoryzowanego dostępu do informacji? (Wybierz dwa.)

A. Zanieczyszczenie parametru

B. Wykorzystywanie niezabezpieczonych bezpośrednich odwołań do obiektów

C. Atak cross-site scripting

D. Fałszerstwo żądań między witrynami

E. Atak przekierowania

65. Która forma ataku typu cross-site scripting (XSS) wykorzystuje starszą, podatną na ataki przeglądarkę internetową uruchomioną lokalnie na komputerze ofiary?

A. Przechowywane/trwałe

B. Clickjacking

C. Odbite

D. Obiektowy Model Dokumentu (DOM)

66. W ramach testu penetracyjnego szarej skrzynki musisz stworzyć skrypt Pythona, aby uruchomić exploita przeciwko docelowej organizacji. W ramach skryptu musisz dokonać porównania między dwiema zmiennymi, które sprawdza, czy nie są równe. Jakich operatorów relacyjnych możesz użyć? (Wybierz dwa.)

A. <>

B. ==

C. -eq

D. !=

E.-ne

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

A. =

B. ==

C. -eq

D. !=

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

A. =

B. ==

C. -eq

D. !=

69. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt Bash, aby uruchomić exploita przeciwko docelowej organizacji. W ramach skryptu musisz dokonać porównania między dwiema zmiennymi całkowitymi, aby sprawdzić, czy jedna jest liczbowo większa od drugiej. Którego operatora relacji powinieneś użyć?

A. >

B. <

C. -gt

D. !>

70. Którego operatora relacyjnego można użyć zarówno w Pythonie, jak i Ruby, aby sprawdzić, czy jedna wartość jest liczbowo większa od drugiej?

A. >

B. <

C. -gt

D. !>

71. Właśnie zakończyłeś test penetracyjny dla klienta. Podczas testu mogłeś uzyskać dostęp do serwerowni, podszywając się pod technika dostawcy IT. Udało Ci się podłączyć laptopa do złącza szeregowego routera Cisco w organizacji i uzyskać dostęp do jego konfiguracji. Co powinieneś polecić klientowi w swoim raporcie końcowym, aby rozwiązać ten problem? (Wybierz dwa.)

A. Wyłącz DHCP w sieci przewodowej.

B. Uruchom polecenie enable secret na routerze.

C. Wdrożyć procedury weryfikacji przedstawicieli dostawców.

D. Zaimplementuj filtrowanie adresów MAC na routerze.

72. Przeprowadzając test penetracyjny dla klienta, chcesz mieć pewność, że proces czyszczenia po zaangażowaniu przebiega gładko. Co powinieneś zrobić, aby to osiągnąć?

A. Dokładnie udokumentuj wszystko, co robisz podczas przeprowadzania testu.

B. Twórz tylne drzwi w krytycznych systemach, aby później mieć do nich łatwy dostęp.

C. Utwórz obrazy wszystkich systemów i urządzeń, aby można je było przywrócić do stanu sprzed testu.

D. Usuń wszelkie wpisy dziennika utworzone przez Twoje exploity.

73. Przeprowadzasz proces oczyszczania po zakończeniu zaangażowania po zakończeniu testu penetracyjnego. Co powinieneś zrobić? (Wybierz dwa.)

A. Usuń wszystkie sesje powłoki utworzone podczas testu.

B. Ukryj przed klientem wszystko, co zrobiłeś podczas testu.

C. Dokumentuj wszystko, co robisz podczas sprzątania.

D. Ukryj wszystko, co robisz, aby posprzątać po teście.

74. Przeprowadzasz proces czyszczenia po zakończeniu zaangażowania po zakończeniu testu penetracyjnego. Co powinieneś zrobić?

A. Poproś klienta o podpisanie umowy o nieujawnianiu technik, których użyłeś podczas testu.

B. Usuń wszelkie poświadczenia utworzone przez testera użyte podczas testu.

C. Napisz krytykę błędów, które popełnili wewnętrzni administratorzy podczas testu.

D. Ukryj przed klientem wszystko, co zrobiłeś podczas testu.

75. Po zakończeniu testu penetracyjnego przeprowadzasz proces czyszczenia po zaangażowaniu. Co powinieneś zrobić?

A. Usuń wszelkie narzędzia lub programy narzędziowe zainstalowane podczas testu.

B. Zresetuj wszystkie poświadczenia administracyjne do ich wartości domyślnych.

C. Zresetuj wszystkie zapory do konfiguracji domyślnych.

D. Zainstaluj ponownie wszystkie usługi sieciowe, korzystając z ustawień domyślnych.

76. Do czego służy obiektowy model dokumentu (DOM) w przeglądarce internetowej użytkownika?

A. Strukturyzacja treści w przeglądarce

B. Przekazywanie wiadomości innym podmiotom

C. Przechowywanie zaszyfrowanych wartości, po których następuje znak „#”

D. Pomoc w łagodzeniu ataków XSS

77. Jaki jest cel poniższego kodu PHP?

```
do {
$data = fread($handle, 8192);
if (strlen($data ==0) {
Break’
}
echo($data);
}while (true);
```

A. Tworzy pętlę wyświetlającą echa zawartości $data, aż osiągnie ona długość 0

B. Tworzy pętlę, deklaruje $data i weryfikuje rozmiar zmiennej

C. Tworzy pętlę, która odbija zawartość danych

D. Tworzy pętlę, ale zabija proces, jeśli dane są mniejsze niż 8192 bajtów

78. Która z poniższych opcji może być identyfikatorem IDOR, biorąc pod uwagę następujące adresy URL? (Zaznacz wszystkie pasujące odpowiedzi).

A. http://example.com/index.php?emp_id=12345

B. http://example.com/index.php

C. http://example.com/sales.php?acct=4532345

D. http://example.com/profile.php?state=CA&zip=90001

79. _____ jest unikalny i służy do identyfikacji każdej instancji usługi Windows. W systemie Windows Kerberos wymaga tego aby

_____ był powiązany z co najmniej jednym kontem logowania do usługi (tj. kontem, na którym działa usługa).

A. Nazwa hosta

B. Nazwa domeny

C. Unikalny identyfikator

D. Główna nazwa usługi

80. Podczas pentestu używasz polecenia wmic do identyfikowania niecytowanych ścieżek usług. Udało Ci się znaleźć ścieżkę w C:\Program Files (x86)\data\shared files\vulnerable.exe i użyłeś accesschk.exe, aby stwierdzić, że masz uprawnienia do zapisu w katalogu „data”. Aby eskalować uprawnienia przy następnym uruchomieniu usługi, musisz określić plik wykonywalny, który będzie wykonywany w ścieżce usługi. Jaka jest prawidłowa nazwa pliku wykonywalnego który powinieneś stworzyć?

A. shared.exe

B. files.exe

C. Files.exe

D. Program.exe