1. D i E. Zaawansowane trwałe zagrożenie (APT) to długotrwały atak ukierunkowany, w którym atakujący uzyskuje dostęp do sieci i pozostaje tam niewykryty przez dłuższy czas. W związku z tym tylko zorganizowana przestępczość lub podmiot państwa narodowego może mieć poziom zaawansowania i fundusze wymagane do przeprowadzenia takiego ataku. Dzieciakom skryptowym, haktywistom i złośliwym informatorom zazwyczaj brakuje wiedzy technicznej i/lub funduszy niezbędnych do przeprowadzenia APT.

2. A i C. Zaawansowane trwałe zagrożenia (APT) są zazwyczaj wymierzone w cele o wysokiej wartości, takie jak rządy, kontrahenci w dziedzinie obronności, organizacje międzynarodowe i organizacje finansowe. Internetowe witryny edukacyjne, gabinety dentystyczne, a nawet uczelnie społeczne zazwyczaj nie są wystarczająco wartościowe jako cele, aby uzasadnić APT.

3. B. Ataki haktywistów są zwykle motywowane politycznie, a nie finansowo. Złośliwy insider jest zwykle motywowany zemstą lub zyskiem finansowym. Działacz przestępczości zorganizowanej jest najprawdopodobniej motywowany korzyściami finansowymi. Scenariusz może mieć różne motywacje, takie jak rozgłos.

4. B. Dzieciak skryptowy może mieć różne motywacje. Jednym z najczęstszych jest uwaga. Często chwalą się swoimi wyczynami na forach internetowych i w mediach społecznościowych. Złośliwy insider jest zwykle motywowany zemstą lub zyskiem finansowym. Działacz przestępczości zorganizowanej jest najprawdopodobniej motywowany korzyściami finansowymi. Państwo narodowe jest najprawdopodobniej motywowane celami politycznymi lub militarnymi.

5. D. Ponieważ ocena białoskrzynkowa dostarcza testerom penetracyjnym obszernych informacji na temat celu, zwykle zapewnia najdokładniejszą ocenę i zazwyczaj wymaga jak najmniej czasu na przeprowadzenie. Test szarej skrzynki to połączenie testów czarnej i białej skrzynki. W związku z tym przeprowadzenie testu trwa dłużej, ponieważ testerzy muszą odkryć więcej informacji. W teście czarnoskrzynkowym testerzy nie mają dostępu ani informacji o środowisku docelowym, co sprawia, że ocena jest znacznie mniej kompletna i jej przeprowadzenie trwa znacznie dłużej. Oceny oparte na celach lub obiektywnych są zwykle zaprojektowane do oceny ogólnego bezpieczeństwa organizacji.

6. B i C. Narzędzie whois może służyć do zbierania informacji o własności domeny z rejestrów publicznych. Narzędzie recon-ng to modułowa struktura rozpoznania sieci WWW, która organizuje i zarządza informacjami OSINT.

7. A. Narzędzie whois może służyć do zbierania informacji o własności domeny z rejestrów publicznych. W przykładzie pokazanym w tym pytaniu możesz dowiedzieć się, kto jest rejestratorem domeny, nazwę organizacji, która jest jej właścicielem, adres organizacji, numer telefonu organizacji, imię i nazwisko pracownika zarządzającego domeną oraz adres e-mail tego pracownika.

8. B. Narzędzie nslookup może być użyte do tłumaczenia nazwy domeny na powiązany z nią adres IP.

9. D. Narzędzie recon-ng zapewnia strukturę rekonesansu sieci, która umożliwia prowadzenie rekonesansu typu open source na temat organizacji w sieci. W tym przykładzie zostały wyświetlone wszystkie publiczne serwery skojarzone z nazwą domeny określoną wraz z ich adresami IP.

10. B. Domyślnym portem dla usługi przekazywania poczty SMTP jest port 25. Większość dystrybucji Linuksa używa demona poczty e-mail, takiego jak sendmail, do wewnętrznego przesyłania wiadomości. Można go jednak również używać do wysyłania wiadomości przez sieć za pośrednictwem protokołu SMTP na porcie 25. Normalnie ten port jest chroniony zaporą ogniową na serwerze publicznym, aby uniemożliwić wykorzystanie demona do nieautoryzowanego przekazywania wiadomości e-mail przez

spamerów. Czasami możesz znaleźć serwery, na których ktoś otworzył port 25 i zapomniał go zamknąć, co sprawia, że host jest podatny na ataki.

11. A. Przesłuchanie polega na przesłuchaniu pracownika organizacji docelowej, wykorzystując strach jako motywację do zbierania informacji. Przesłuchanie nie jest techniką zwykle stosowaną przez testerów penetracyjnych, ponieważ prawdopodobnie doprowadziłoby do postawienia testerowi zarzutów karnych, jak również postępowania cywilnego.

12. B i D. Podszywanie się to technika socjotechniki, którą penetrator może wykorzystać do uzyskania fizycznego dostępu do obiektu celu. W tym scenariuszu recepcjonistka zezwoliła testerowi na dostęp do obiektu organizacji, ponieważ tester wydaje się pochodzić od zaufanego dostawcy. Tester wykorzystał również exploita do upuszczania klucza USB, mając nadzieję, że użytkownik włoży dysk flash do swojego komputera i zainstaluje zawarte w nim złośliwe oprogramowanie.

13. C. Tester penetracyjny wykorzystał w tym scenariuszu techniki „shoppingu na ramieniu". W shoulder surfing tester obserwuje informacje, które pracownicy wpisują lub wyświetlają na swoich komputerach, próbując zebrać poufne informacje. Na przykład tester może użyć funkcji Shoulder surfing do zebrania nazw użytkowników, haseł, adresów e-mail, numerów telefonów, nazw udziałów serwerów plików i tak dalej.

14. D i E. Tester penetracyjny wykorzystał w tym scenariuszu techniki „shopping surfingu" i biznesowej poczty elektronicznej. W shoulder surfing tester obserwuje informacje, które pracownicy wpisują lub wyświetlają na swoich komputerach, próbując zebrać poufne informacje. W tym przykładzie tester skorzystał z funkcji Shoulder surfing, aby zebrać nazwę użytkownika poczty e-mail i hasła pracownika. Tester następnie wykorzystał zhakowane konto, aby zebrać informacje od innych pracowników. Nazywa się to złamaniem biznesowej poczty e-mail.

15. B. To jest przykład pozyskiwania. Zdobywając zaufanie pracowników, tester był w stanie wydobyć od nich poufne informacje na temat pracodawcy.

16. D. Gdy nmap wskazuje, że port jest filtrowany, zwykle oznacza to, że skojarzona usługa jest zainstalowana i uruchomiona, ale zapora hosta blokuje port.

17. B. Gdy nmap wskazuje, że port jest otwarty, zwykle oznacza to, że skojarzona usługa jest zainstalowana, działa i jest dostępna przez zaporę hosta.

18. A. Gdy nmap wskazuje, że port jest zamknięty, zwykle oznacza to, że powiązana usługa nie jest w ogóle zainstalowana lub została zainstalowana, ale obecnie nie jest uruchomiona. Dlatego nic nie nasłuchuje na skojarzonym porcie.

19. A. Opcja –sS powoduje, że nmap uruchamia skanowanie TCP SYN. Podczas tego skanowania nmap wysyła pakiet TCP SYN do hosta docelowego, a następnie host docelowy odpowiada pakietem SYN ACK. Jednak zamiast zakończyć połączenie, nmap wysyła pakiet resetujący do hosta docelowego.

20. D. Wszystkie opcje pokazane w tym pytaniu spowodują, że nmap wykryje usługi działające na hoście docelowym. Jednak tylko opcja –sV może być używana z nmapem do wykrywania numeru wersji tych usług.

21. D. Wskaźnik wcześniejszego uruchomienia komunikacji z włamaniem ma miejsce, gdy tester penetracyjny odkryje, że sieć lub system został już wcześniej naruszony przez innego atakującego. W takiej sytuacji tester zazwyczaj komunikuje odkrycie klientowi natychmiast, zamiast czekać na zakończenie testu.

22. D. Wyzwalacz komunikacji etapów ma miejsce, gdy test penetracyjny przechodzi z jednej fazy do drugiej.

23. B. Wskaźnik wcześniejszego uruchomienia komunikacji z włamaniem ma miejsce, gdy tester penetracyjny odkryje, że sieć lub system został już wcześniej naruszony przez innego atakującego. W takiej sytuacji tester zazwyczaj komunikuje odkrycie klientowi natychmiast, zamiast czekać na zakończenie testu.

24. B. Wyzwalacz komunikacji o krytycznych ustaleniach ma miejsce, gdy tester penetracyjny odkryje lukę w zabezpieczeniach tak poważną, że należy ją natychmiast rozwiązać, zamiast czekać na zakończenie testu.

25. C. Wyzwalacz komunikacji etapów ma miejsce, gdy test penetracyjny przechodzi z jednej fazy do drugiej.

26. A i D. Przykładowe żądania aplikacji są zwykle wykorzystywane do testowania aplikacji (komputerowych lub internetowych), które zostały opracowane we własnym zakresie. Aplikacje opracowane we własnym zakresie zwykle nie są poddawane takiemu samemu poziomowi kontroli, jak aplikacje komercyjne, co czyni je możliwymi wektorami ataku, które można wykorzystać. Przykładowe żądania aplikacji nie są generalnie wymagane w przypadku aplikacji komercyjnych, takich jak Word, Excel czy Photoshop, ponieważ ich słabości są już dobrze udokumentowane.

27. C. Aplikacje opracowane wewnętrznie zwykle nie są poddawane takiemu samemu poziomowi kontroli jak aplikacje komercyjne, co czyni je możliwymi wektorami ataku, które można wykorzystać. Na przykład podczas generowania żądań aplikacji przykładowych większość testerów penetracyjnych rzuca nieoczekiwane informacje do aplikacji opracowanych wewnętrznie, aby zobaczyć, jak aplikacja odpowiada. Na przykład może się okazać, że wprowadzenie bardzo długiego ciągu tekstowego w polu, które oczekuje tylko ośmiu znaków, może wygenerować błąd przepełnienia bufora. Możesz następnie użyć tego słabego zachowania w zakresie obsługi błędów, aby wstawić i uruchomić złośliwy kod na serwerze sieciowym, na którym znajduje się aplikacja.

28. A. Simple Object Access Protocol (SOAP) to specyfikacja protokołu przesyłania komunikatów, która definiuje sposób wymiany informacji strukturalnych między aplikacjami internetowymi. Pliki projektu SOAP można tworzyć z plików WSDL (Web Services Description Language).

29. D. Swagger to platforma open source zaprojektowana, aby pomóc programistom w projektowaniu, budowaniu, dokumentowaniu i testowaniu usług internetowych Representational State Transfer (REST). REST jest alternatywą dla protokołu SOAP. W rzeczywistości REST zaczął zastępować SOAP jako platformę wybieraną w większości nowoczesnych aplikacji internetowych.

30. B. Architektura aplikacji internetowej Representational State Transfer (REST) jest oparta na protokole Hypertext Transfer Protocol (HTTP).

31. D. National Vulnerability Database (NVD) jest utrzymywany przez Narodowy Instytut Nauki i Technologii rządu USA. Dostęp do NVD można uzyskać pod adresem https://nvd .nist.gov. Ta witryna internetowa zawiera podsumowanie aktualnych luk w zabezpieczeniach uszeregowanych według ich wagi.

32. C. Baza danych Common Vulnerabilities and Exposures (CVE) jest zasobem opracowanym przez społeczność, do którego można uzyskać dostęp pod adresem http://cve.mitre.org. Baza danych CVE zawiera listę publicznie znanych luk w zabezpieczeniach cybernetycznych. Ilekroć dostawca w dowolnym miejscu na świecie odkryje lukę w swoim produkcie, dodaje wpis do bazy danych CVE.

Celem jest stworzenie wspólnego zasobu, z którego każdy może korzystać, zamiast utrzymywania przez każdego pojedynczego producenta własnej bazy danych zawierającej tylko luki w zabezpieczeniach związane z ich produktami.

33. C. Baza danych Common Weakness and Enumeration (CWE) jest zasobem opracowanym przez społeczność, do którego można uzyskać dostęp pod adresem http://cwe.mitre.org. Baza danych CWE zawiera listę publicznie znanych luk w zabezpieczeniach cybernetycznych związanych ogólnie z oprogramowaniem, a nie z konkretnym produktem.

34. D. Wspólny wzorzec ataku, wyliczenie i klasyfikacja

Baza danych (CAPEC) jest zasobem opracowanym przez społeczność, do którego można uzyskać dostęp pod adresem http://capec.mitre.org. Baza danych CAPEC zawiera katalog powszechnie stosowanych wzorców cyberataków.

35. B. Full Disclosure to źródło badań typu open source, publikowane przez tę samą organizację, która produkuje narzędzie nmap. Można go uzyskać pod adresem www.seclists.org/fulldisclosure.

36. B. Wykorzystanie otwartej usługi SMTP do wysyłania nieautoryzowanych wiadomości e-mail nazywa się przekaźnikiem SMTP. Większość nowych systemów ma przepisy, które mają temu zapobiec, ale wiele starszych systemów serwerowych tego nie robi.

37. A. Jednym ze sposobów wykorzystania otwartej usługi SMTP do wysyłania nieautoryzowanych wiadomości e-mail jest połączenie się z adresem IP serwera SMTP na porcie 25 za pomocą klienta Telnet. Po nawiązaniu połączenia możesz użyć interfejsu wiersza poleceń do tworzenia i wysyłania wiadomości.

38. A i B. Domyślnie serwer FTP używa dwóch portów: 20 i 21. Port 20 służy do przesyłania danych między serwerem FTP a klientem FTP. Port 21 służy do przesyłania poleceń między klientem FTP a serwerem FTP.

39. C. Jedną z kluczowych słabości protokołu FTP jest fakt, że przesyła on wszystkie dane między serwerem FTP a klientem FTP w postaci zwykłego tekstu, w tym dane uwierzytelniające. Sniffowanie ruchu FTP umożliwia przechwytywanie nazw użytkowników i haseł FTP. Niektóre implementacje serwera FTP wykorzystują istniejące sieciowe konta użytkowników i hasła do uwierzytelniania połączeń FTP. Tak więc, przechwytując dane uwierzytelniające FTP, możesz potencjalnie przechwycić również wewnętrzne konta użytkowników sieci i hasła.

40. A. To jest przykład zatrucia DNS. Ten exploit wykorzystuje zaufanie użytkowników do adresu URL, który wydaje się prawidłowy. Ponieważ użytkownicy wprowadzają prawidłowy adres URL, nie mają pojęcia, że wykorzystywany jest exploit. Jednak sam serwer DNS został przekonfigurowany w celu rozwiązania nazwy domeny w adresie URL na adres IP złośliwego serwera.

41. A. Chociaż Nikto jest zwykle uważany za skaner podatności używany przez testerów penetracyjnych, może być również używany przez administratorów systemu do weryfikacji zgodności konfiguracji w ich sieciach, w szczególności z konfiguracją ich serwerów internetowych.

42. D. Narzędzie proxychains pozwala na wykonanie zadań testów penetracyjnych przeciwko docelowej organizacji i sprawienie, by generowany ruch sieciowy wyglądał, jakby pochodził z pośredniczącego systemu proxy.

43. A i D. Zarówno APK Studio, jak i APKX mogą być używane do debugowania, a nawet dekompilacji pliku wykonywalnego Androida.

44. A i D. Zarówno AFL, jak i Peach mogą być używane do wykonywania fuzzingu aplikacji w ramach gwarancji oprogramowania.

45. A i B. Zarówno Findsecbugs, jak i Yet Another Source Code Analyzer (YASCA) mogą być używane do przeprowadzania statycznych testów bezpieczeństwa aplikacji (SAST) lub dynamicznych testów bezpieczeństwa aplikacji (DAST) w ramach zapewniania oprogramowania.

46. C. Ustawienie zasad grupy „Resetuj licznik blokady konta po" określa, ile czasu musi upłynąć po nieudanej próbie logowania, zanim licznik nieudanych prób logowania zostanie zresetowany do 0. To ustawienie zasad pomaga zapobiegać atakom siłowym poprzez znaczne zwiększenie czas potrzebny do przeprowadzenia ataku.

47. A. Polecenie chage może być używane w systemach Linux do automatycznego blokowania kont użytkowników po określonym czasie. Zapobiega to wykorzystywaniu przestarzałych kont użytkowników przez atakującego lub niezadowolonego byłego pracownika w celu uzyskania nieautoryzowanego dostępu.

48. A. Polityka „Przechowuj hasła przy użyciu odwracalnego szyfrowania" jest wysoce niepewna. Jest dołączona do nowoczesnych wdrożeń, aby zapewnić zgodność wsteczną ze starszymi aplikacjami. Klient, który ma włączoną tę zasadę, powinien zostać poinformowany o konsekwencjach dotyczących bezpieczeństwa i rozważyć uaktualnienie do nowszych aplikacji, które tego nie wymagają.

49. B. Ponieważ aplikacja została opracowana we własnym zakresie, klient powinien mieć możliwość przepisania kodu tak, aby hasła były szyfrowane przez aplikację przed zapisaniem ich w bazie danych.

50. A. Polecenia chage można użyć w systemach Linux do skonfigurowania przedawniania haseł dla kont użytkowników. Na przykład może służyć do zablokowania konta użytkownika, jeśli użytkownik nie zmieni swojego hasła po określonej liczbie dni.

51. C i D. Standard PCI-DSS wymaga, aby organizacje zajmujące się przetwarzaniem kart kredytowych przeprowadzały zarówno wewnętrzne, jak i zewnętrzne testy penetracyjne przynajmniej raz w roku. W razie potrzeby mogą je wykonywać częściej, ale nie są do tego zobowiązani. Organizacje te muszą również przeprowadzać testy penetracyjne po dokonaniu istotnych zmian w infrastrukturze sieciowej.

52. A. Ta dyskusja powinna mieć miejsce w fazie planowania i określania zakresu. Firma wykonująca testy penetracyjne i klient powinni uzgodnić zasady zakończenia oceny przed rozpoczęciem testu. Informacje te powinny były zostać zapisane w pisemnym oświadczeniu o pracy (SOW), które jasno określało narzędzia i techniki, z których mogli korzystać testerzy penetracji, oraz ryzyko związane z ich użyciem.

53. D. Deklaracja pracy (SOW) jest umową, którą należy określić na etapie planowania i określania zakresu testu penetracyjnego. Zawiera umowę roboczą pomiędzy testerem penetracyjnym a klientem, która określa konkretne techniki, narzędzia, czynności, produkty i harmonogramy testu. Może być używany w połączeniu z istniejącą główną umową o świadczenie usług (MSA).

54. D. Test penetracyjny białej skrzynki zapewnia pełny dostęp do sieci wewnętrznej, w tym ustawienia konfiguracji kluczowych urządzeń infrastruktury, takich jak routery, przełączniki, punkty dostępowe i serwery. Z tego powodu testy białej skrzynki są czasami nazywane testami pełnej wiedzy, ponieważ zapewniają pełny dostęp i widoczność.

55. A. Umowa o zachowaniu poufności (NDA) to umowa prawna, która chroni informacje, które wykonawca może odkryć podczas testu penetracyjnego. Zabrania wykonawcy ujawniania takich informacji osobom nieuprawnionym.

56. D. Sprzęt produkcyjny SCADA jest o wiele bardziej wrażliwy niż tradycyjne zasoby sieciowe, takie jak serwery i routery. Zwykle trudno nimi zarządzać, aktualizować i chronić przed exploitami. W związku z tym mogą być również podatne na skanowanie luk w zabezpieczeniach i mogą przejść w tryb offline podczas procesu skanowania.

57. A. Okna czasowe, w których najczęściej można uruchomić skanowanie pod kątem luk skutecznie są pod silnym wpływem wymagań prawnych, szczytowych czasów ruchu i ograniczeń sprzętowych. Z drugiej strony wewnętrzny personel IT najprawdopodobniej nie będzie zaangażowany w przeprowadzanie skanowania podatności podczas testu penetracyjnego.

58. B. W tym scenariuszu ma miejsce statyczna analiza kodu (zwana również analizą kodu źródłowego). W tego typu teście tester uzyskuje dostęp do kodu źródłowego aplikacji i sprawdza go pod kątem słabości, które można wykorzystać. Oczywiście tester musi mieć solidne przygotowanie programistyczne, aby móc wykonać tego rodzaju recenzję.

59. A. Fuzzing występuje, gdy tester wysyła losowe, nieoczekiwane informacje do danych wejściowych aplikacji, aby zobaczyć, jak zareaguje. Na przykład tester może próbować wykonać exploit przepełnienia bufora, wysyłając zbyt duże dane wejściowe zawierające kod wykonywalny. Jeśli aplikacja nie obsługuje poprawnie złośliwych danych wejściowych, możliwe jest zapisanie kodu wykonywalnego w pamięci RAM systemu docelowego, a następnie wykonanie go przez atakującego.

60. C. Ponieważ jest to serwer o znaczeniu krytycznym, dobrym pomysłem może być uruchomienie skanowania testowego w środowisku laboratoryjnym przed skanowaniem działającego systemu. Pomoże to testerowi ocenić wpływ skanowania przed uruchomieniem go na aktywnym systemie.

61. C i E. Włączenie pliku to exploit, który umożliwia testerowi przesłanie pliku (zazwyczaj zawierającego złośliwy kod) do aplikacji internetowej. Plik może być lokalny lub znajdować się w zdalnej witrynie internetowej. Jest to tak naprawdę forma ataku typu injection i tak jak w przypadku każdego ataku typu injection, walidacja danych wejściowych ze strony programisty aplikacji internetowej jest kluczem do zapobieżenia temu.

62. A i E. Chociaż komentowanie kodu źródłowego aplikacji jest najlepszą praktyką dla programistów, może również tworzyć luki w zabezpieczeniach, ponieważ zapewnia atakującemu (lub testerowi penetracji), który przegląda kod źródłowy, obszernych informacji na temat działania aplikacji. Podobnie dostarczanie zbyt pełnych komunikatów o błędach może być najlepszą praktyką podczas programowania aplikacji, ale pozostawienie ich w wydanej aplikacji może dostarczyć atakującemu cenne informacje.

63. C i D. Programista powinien dołączyć procedury, które mówią aplikacji, co ma zrobić, jeśli napotka błąd. Na przykład wiele ataków polegających na przepełnieniu bufora wykorzystuje aplikacje, które nie wiedzą, jak zareagować, gdy otrzymują więcej informacji, niż się spodziewały. Podobnie wszystkie aplikacje powinny mieć swój kod podpisany cyfrowo. Ujawni to wszelkie nieautoryzowane modyfikacje dokonane w kodzie.

64. D. Programista w tym scenariuszu użył poświadczeń zakodowanych na stałe. Jeśli atakujący (lub tester penetracyjny) miałby wyświetlić kod źródłowy aplikacji, miałby dostęp do poświadczeń uwierzytelniania bazy danych.

65. C. Programista w tym scenariuszu użył ukrytych elementów w kodzie HTML. Jest to niezabezpieczona praktyka kodowania, która może skutkować przechowywaniem poufnych informacji w przeglądarce użytkownika (DOM).

66. C. Operatora relacyjnego -le można użyć zarówno w Bash, jak i PowerShell do sprawdzenia, czy jedna wartość jest liczbowo mniejsza lub równa drugiej.

67. A. Operator relacyjny <= może być użyty zarówno w Pythonie, jak i Ruby do sprawdzenia, czy jedna wartość jest liczbowo mniejsza lub równa drugiej.

68. B. Dodanie odczytanej linii TargetHost do skryptu Bash powoduje, że akceptuje on dane wprowadzone w wierszu poleceń przez użytkownika i przypisuje je do zmiennej o nazwie TargetHost.

69. A. Dodanie linii echo $TargetHost do skryptu Bash powoduje wyświetlenie na ekranie wartości zmiennej o nazwie TargetHost.

70. C. Polecenie test może być użyte z poziomu struktury sterowania przepływem jeśli/to, aby ocenić, czy określony warunek jest prawdziwy.

71. A i B. Mogą to być chwile, które wymagają natychmiastowej komunikacji z klientem. Poniżej przedstawiono niektóre typowe wyzwalacze komunikacji związane z testami penetracyjnymi. Wyzwalacze komunikacji powinny być wykonywane po zakończeniu fazy testowania, odkryciu krytycznego odkrycia lub odkryciu wskaźników poprzedniego kompromisu. W tym scenariuszu chcielibyśmy skontaktować się z klientem, jeśli system stanie się niedostępny po próbie testu i jeśli system wykaże oznaki wcześniejszego nieautoryzowanego dostępu.

72. D. W tym scenariuszu klient nie ma budżetu, aby natychmiast naprawić wszystkie znalezione luki w zabezpieczeniach. W takim przypadku najlepszą sugestią, aby powiedzieć klientowi, jest najpierw naprawienie najbardziej krytycznej luki, a następnie, gdy fundusze staną się dostępne, naprawienie innych krytycznych luk.

73. A. W tym scenariuszu, ponieważ istnieje kilka portów o wysokim numerze nasłuchujących na publicznym serwerze WWW. Najlepszym zaleceniem byłoby wyłączenie niepotrzebnych usług, ponieważ klient korzysta tylko z wersji 443. Niepotrzebne usługi mogą stanowić zagrożenie dla bezpieczeństwa, ponieważ zwiększają powierzchnię ataku, zapewniając potencjalnemu napastnikowi dodatkowe sposoby na próbę wykorzystania systemu.

74. C. Wzmacnianie systemu, znane również jako wzmacnianie systemu operacyjnego, pomaga zminimalizować luki w zabezpieczeniach. Celem wzmocnienia systemu jest pozbycie się jak największej liczby zagrożeń bezpieczeństwa. Zwykle odbywa się to poprzez usunięcie z komputera wszystkich nieistotnych programów i narzędzi. Cel utwardzania systemów poprzez usuwanie nieużywanych programów, funkcji kont, aplikacje, porty, uprawnienia, dostęp itp. powodują, że atakujący mają mniej możliwości uzyskania dostępu do Twojej sieci. Istnieje kilka rodzajów działań wzmacniających system. Należą do nich:

■ Utwardzanie aplikacji

■ Hartowanie systemu operacyjnego

■ Utwardzanie serwera

■ Utwardzanie bazy danych

■ Utwardzanie sieci

75. B, E i G. W tej sytuacji, ponieważ tester był w stanie skompromitować pojedynczą stację roboczą i jest w stanie poruszać się na boki przez sieć, najlepsze zalecenia dla klienta byłyby następujące:

■ Użyj uwierzytelniania wieloskładnikowego. Uwierzytelnianie wieloskładnikowe (MFA) to metoda uwierzytelniania, w której użytkownik komputera uzyskuje dostęp dopiero po pomyślnym przedstawieniu dwóch lub więcej dowodów (lub czynników) mechanizmowi uwierzytelniania.

■ Zwiększ minimalną złożoność hasła. Złożone hasła wykorzystują różne typy znaków w unikalny sposób, aby zwiększyć bezpieczeństwo, co utrudnia atakującemu złamanie.

■ Włącz szyfrowanie całego dysku. Szyfrowanie całego dysku (FDE) to szyfrowanie na poziomie sprzętowym. FDE działa poprzez automatyczną konwersję danych na dysku twardym do postaci, której nie może zrozumieć nikt, kto nie ma klucza do „cofnięcia" konwersji.

76. C. Polecenie pull służy do pobierania plików z urządzenia, natomiast polecenie push może służyć do przesyłania plików do urządzenia.

77. D. Dostawcy treści mogą zapewnić punkt wstrzykiwania z poziomu aplikacji. Niektóre aplikacje mobilne współdzielą te same lokalizacje pamięci zewnętrznej. W związku z tym, jeśli punkt wstrzykiwania może zostać wykorzystany, może to umożliwić złośliwemu użytkownikowi odczytanie treści poza środowiskiem piaskownicy aplikacji.

78. A. Python jest zorientowany obiektowo, tak że wszystko jest traktowane jako obiekt.

79. A. Właściwym sposobem dziedziczenia modułu z klasy jest najpierw określenie modułu, z którego chcesz dziedziczyć klasę, a następnie klasy z modułu. Z modułu importuje klasę. W ten sposób nie musisz ładować całego modułu - tylko te klasy, których potrzebujesz.

80. B. Gdy klient dostarczy potwierdzenie pomyślnego dostarczenia i wydobycia raportu, zespół testowy powinien rozważyć przechowywanie pojedynczej cyfrowej kopii raportu w zaszyfrowanym sejfie, aby zapobiec nieautoryzowanemu ujawnieniu. Wszystkie pozostałe cyfrowe lub pisemne kopie raportu należy oznaczyć do właściwego usunięcia i usunięcia, w oparciu o uzgodnione metody opisane w RoE.