1. A i E. Dokument zakresu musi określać m.in. dlaczego test jest wykonywany i kim jest grupa docelowa. W razie potrzeby można uwzględnić inne opcje wymienione w tym pytaniu, ale nie są one wymagane.

2. A i B. Zasady zaangażowania (ROE) powinny zawsze zawierać harmonogram zaangażowania, a także przegląd wszelkich przepisów, które konkretnie regulują cel, aby upewnić się, że ich nie złamiesz. Lista innych organizacji, które przetestowałeś w przeszłości, lub lista konkurentów docelowej organizacji prawdopodobnie nie zostanie określona w zasadach zaangażowania. Szczegółowa mapa sieci celu prawdopodobnie nie zostanie uwzględniona w teście czarnej lub szarej skrzynki.

3. B i C. ROE powinno określać, które lokalizacje, systemy, aplikacje lub inne potencjalne cele są objęte lub wykluczone z testu. Powinno to identyfikować wszystkich zewnętrznych dostawców usług, na których test może mieć wpływ, takich jak dostawcy usług internetowych, dostawcy usług w chmurze lub usługi monitorowania bezpieczeństwa. . Procedury rozliczeniowe i arbitrażowe prawdopodobnie zostaną omówione w umowie ogólnej między Tobą a klientem, a nie w ROE. Jest mało prawdopodobne, że klient będzie chciał, abyś powiadomił swoich konkurentów, że testujesz ich zabezpieczenia.

4. B i E. ROE powinno określać, kiedy iw jaki sposób nastąpi komunikacja między Tobą a klientem. Czy powinieneś dostarczać codzienne lub cotygodniowe aktualizacje, czy po prostu poinformujesz o zakończeniu testu? ROE powinno również określać zachowania dozwolone ze strony celu. Na przykład angażowanie się w zachowania obronne, takie jak unikanie lub umieszczanie na czarnej liście, może ograniczyć wartość testu.

5. C. Zgoda ustna jest zwykle uważana za niewystarczającą. Przed rozpoczęciem testu penetracyjnego musisz uzyskać podpisaną umowę z kierownictwem wyższego szczebla, która zezwala na przeprowadzenie testu. Umowa ta będzie funkcjonować jako karta „wyjdź z więzienia za darmo", jeśli twoje działania zostaną zgłoszone władzom. Pozostałe parametry opisane w tym scenariuszu zostały odpowiednio zdefiniowane.

6. D. Domyślny port dla usługi SMB/CIFS przy użyciu bezpośredniego połączenia TCP do portu 445. Do udostępniania plików używany jest protokół SMB/CIFS, więc dany host musi być serwerem plików.

7. C. Domyślny port dla usługi Telnet to 23. Telnet służy do zdalnego zarządzania systemem za pomocą interfejsu wiersza poleceń. Telnet to bardzo stary i niezabezpieczony protokół. Wszystkie informacje przesyłane między serwerem Telnet a klientem są przesyłane w postaci niezaszyfrowanej, w tym informacje dotyczące uwierzytelniania. Podsłuchując ruch przychodzący i wychodzący z tego hosta na porcie 23, możesz być w stanie przechwycić nazwy użytkowników i hasła.

8. B. Domyślne porty używane przez usługę FTP to 20 i 21. FTP służy do przesyłania plików między hostami za pośrednictwem połączenia sieciowego. FTP to bardzo stary i niezabezpieczony protokół. Wszystkie informacje przesyłane między serwerem FTP a klientem są przesyłane w postaci niezaszyfrowanej, w tym informacje uwierzytelniające. Podsłuchując ruch przychodzący i wychodzący z tego hosta na portach 20 i 21, możesz być w stanie przechwycić nazwy użytkowników i hasła.

9. D. Domyślny port używany przez usługę TFTP to 69. TFTP zapewnia szybki i łatwy sposób przesyłania plików między hostami przez połączenie sieciowe. W przeciwieństwie do FTP, TFTP używa bezpołączeniowego protokołu warstwy transportowej UDP zamiast TCP. Brak potwierdzeń pozwala serwerowi TFTP przesyłać pliki szybciej niż serwer FTP. Jednak TFTP jest niezabezpieczonym protokołem. Wszystkie informacje przesyłane między serwerem FTP a klientem są wysłane w postaci

niezaszyfrowanej. Ponadto TFTP nie zapewnia środków do uwierzytelniania połączeń. Dlatego każdy może połączyć się z usługą i przesyłać pliki bez podawania danych uwierzytelniających.

10. A. Kontroler domeny Windows obsługuje wiele usług związanych z domeną. Dlatego większość kontrolerów domeny będzie mieć wiele otwartych portów. Większość będzie zawierać następujące elementy:

Port 88: używany do uwierzytelniania Kerberos.

Port 135: używany do komunikacji między kontrolerami domeny i klientami oraz między kontrolerami domeny.

Porty 138 i 139: używane do replikacji plików między kontrolerami domeny.

Port 389: używany do zapytań LDAP.

Port 445: Używany do udostępniania plików SMB/CIFS.

Port 464: używany do zmiany hasła protokołu Kerberos.

Port 636: Używany do bezpiecznych zapytań LDAP.

Porty 3268 i 3269: używane do komunikacji z Katalogiem globalnym.

Port 53: używany do rozpoznawania nazw DNS.

11. A. Udając kierownika wyższego szczebla, tester penetracyjny w tym przykładzie wykorzystał apel do władz, aby zmusić pracownika do ujawnienia poufnych informacji.

12. D. Udając agenta FBI, tester penetracyjny w tym przykładzie wykorzystał autorytet (i prawdopodobnie strach) jako czynnik motywacyjny, aby zmusić pracownika do ujawnienia poufnych informacji.

13. B. Udając współpracownika znajdującego się w wielkim niebezpieczeństwie w tym scenariuszu, tester penetracyjny stara się zmotywować pracownika do zrezygnowania z nazwy użytkownika i hasła. Może również wykorzystywać sympatię jako czynnik.

14. A. Tester penetracyjny wykorzystuje dowód społeczny jako czynnik motywujący. Ponieważ wydaje się, że ponad 1000 osób miało pozytywne doświadczenia z witryną, większość pracowników prawdopodobnie zaufa witrynie, nawet jeśli poprosi ich o ujawnienie poufnych informacji.

15. D. Tester penetracyjny wykorzystuje niedobór jako czynnik motywujący. Twierdząc, że dostępna jest tylko niewielka liczba urządzeń po drastycznie obniżonej cenie, pracownicy są zmotywowani do dokonania zakupu, zanim skończą się zapasy.

16. C. Polecenie -p U:20,T:21,22 mówi nmapowi, aby po prostu przeskanował port UDP 20 oraz porty TCP 21 i 22. Inne opcje w tym pytaniu również przeskanują te porty; jednak skanują również wiele innych niechcianych portów.

17. A i C. Opcja –p http,https lub opcja –p 80 443 może być użyta z nmapem do przeskanowania hosta w poszukiwaniu usługi serwera WWW.

18. B. Opcja --top-ports 1000 mówi nmapowi, aby skanował domyślne porty używane przez 1000 najpopularniejszych usług sieciowych. Opcja --exclude-ports 53 mówi nmapowi, aby pominął port 53 (domyślny port używany przez serwery DNS) podczas skanowania.

19. C. Opcja -iL nazwa_pliku mówi nmapowi, aby odczytał określony plik i skanował tylko te hosty, które są w nim wymienione.

20. A. Opcja -Pn mówi nmapowi, aby skanował host (lub całą podsieć) bez faktycznego wykrywania hostów. Tego typu skanowania należy unikać podczas testu penetracyjnego, ponieważ zajmuje dużo czasu; skanowany jest każdy port na każdym adresie IP w zakresie, niezależnie od tego, czy adres IP jest prawidłowy. Z tego powodu generuje również ogromny ruch, który może zostać wykryty przez narzędzie IDS lub IPS.

21. B. Wyzwolenie 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.

22. A. Wskaźnik wcześniejszego wyzwolenia 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.

23. B. Zmiana priorytetów celów ma miejsce, gdy klient lub tester decyduje się zmienić ukierunkowanie testu penetracyjnego z uzgodnionego zakresu po rozpoczęciu testu. W tym scenariuszu test PCI DSS jest modyfikowany, aby uwzględnić testowanie pod kątem podatności na nowy typ oprogramowania ransomware.

24. A. Zmiana priorytetów celów ma miejsce, gdy klient lub tester decyduje się zmienić ukierunkowanie testu penetracyjnego z uzgodnionego zakresu po rozpoczęciu testu. W tym scenariuszu składnik czarnej skrzynki został dodany do tradycyjnego testu szarej skrzynki.

25. B. Kiedy normalizujesz dane z testu penetracyjnego, agregujesz wszystkie dane wygenerowane przez wszystkie różne narzędzia i procesy użyte podczas testu i formatujesz je w taki sposób, aby były spójne i łatwe do zrozumienia.

26. A. Język Web Service Description Language (WSDL) to oparty na języku XML język definicji interfejsu, który jest używany do opisywania funkcjonalności oferowanych przez serwer aplikacji WWW, taki jak serwer SOAP. WSDL nie działa dobrze z architekturą aplikacji internetowych Representational State Transfer (REST), która przez lata powoli zastępowała SOAP.

27. B. Język Web Application Description Language (WADL) zapewnia oparty na XML opis usług internetowych opartych na HTTP uruchomionych na serwerze aplikacji internetowej. WADL jest zwykle używany z usługami sieciowymi Representational State Transfer (REST). WADL jest alternatywą dla WSDL i jest ogólnie uważany za łatwiejszy w użyciu, ale brakuje mu również elastyczności związanej z WSDL.

28. B. Definicja schematu XLM (XSD) to specyfikacja W3C, która identyfikuje sposób definiowania elementów w dokumencie XML.

29. D. Przy przeprowadzaniu testu penetracyjnego typu white box, szczególnie takiego, który będzie dotyczył aplikacji opracowanych we własnym zakresie, posiadanie dokumentacji SDK użytego do stworzenia aplikacji może być bardzo pomocne. Diagramy przepływu danych mogą również zapewnić testerom penetracyjnym zrozumienie, w jaki sposób docelowa aplikacja komunikuje się z innymi usługami sieciowymi. Pliki konfiguracyjne mogą zawierać informacje o koncie, adresy IP, klucze API, a nawet hasła.

30. B i D. Podczas przeprowadzania oceny białej skrzynki zazwyczaj chcesz, aby klient umieścił na białej liście konta użytkowników testerów w swoim IPS. Uniemożliwi to ich zablokowanie, gdy zaczną badać obronę. Powinni również skonfigurować wyjątki bezpieczeństwa, które pozwolą systemom testerów penetracyjnych na ominięcie kontroli bezpieczeństwa NAC.

31. D. Każde ze źródeł badań typu open source wymienione w tym pytaniu może zawierać informacje, które można wykorzystać do znalezienia znanych luk w starszej wersji oprogramowania serwera internetowego IIS.

32. A. Baza danych CERT zawiera informacje o ostatnich aktualizacjach zabezpieczeń wydanych przez dostawców oprogramowania i sprzętu oraz opis luk w zabezpieczeniach, którymi mają się zająć.

33. A. Baza danych CAPEC zawiera informacje o znanych wzorcach ataków wykorzystywanych do wykorzystywania słabych punktów, w tym luk w zabezpieczeniach fizycznych.

34. D. Strona internetowa National Vulnerability Database (NVD) zapewnia podsumowanie aktualnych luk w zabezpieczeniach uszeregowanych według ich ważności.

35. A. Baza danych Common Vulnerabilities and Exposures (CVE) jest zasobem opracowanym przez społeczność, który 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. Możesz przeszukać witrynę CVE w celu uzyskania informacji o dodatku SP2 dla serwera 2003.

36. A. Jednym ze sposobów obrony przed zatruciem DNS jest wdrożenie DNSSEC. DNSSEC podpisuje każde żądanie DNS podpisem cyfrowym, aby zapewnić autentyczność. Utrudnia to wstawianie zatrutych rekordów.

37. C. To jest przykład zatruwania pamięci podręcznej DNS. Zamiast naruszać silnie chroniony serwer DNS, tester penetracji po prostu narusza pamięć podręczną DNS na stosunkowo mniej bezpiecznych stacjach roboczych. Efekt netto jest taki sam. Złośliwe oprogramowanie jest powszechnym narzędziem dostarczania exploitów zatruwania pamięci podręcznej DNS.

38. C. Jest to również przykład zatruwania pamięci podręcznej DNS. Zamiast zatruwać lokalną pamięć podręczną DNS na stacjach roboczych, w tym scenariuszu została zatruta pamięć podręczna serwera DNS tylko do buforowania. Zatrute rekordy pozostaną w pamięci podręcznej do momentu osiągnięcia wartości TTL.

39. D. To jest przykład exploita typu pass-the-hash. W przypadku tego exploita tester przechwytuje zaszyfrowane poświadczenia użytkownika NTLM, a następnie ponownie wykorzystuje je do późniejszego uwierzytelnienia w systemie Windows. Ponieważ uwierzytelnianie NTLM wykorzystuje zaszyfrowane dane uwierzytelniające, tester nie musi znać rzeczywistej nazwy użytkownika i hasła ofiary. Zaszyfrowane poświadczenia są wystarczające do utworzenia nowej sesji uwierzytelnionej.

40. B. To jest przykład spoofingu ARP. W tym exploicie tester wysyła fałszywą transmisję ARP w segmencie sieci, która mapuje adres IP legalnego hosta sieciowego na jej adres MAC. W rezultacie cały ruch adresowany do legalnego hosta zostaje przekierowany do systemu testera.

41. C. Narzędzie hashcat można skonfigurować tak, aby używało procesorów graficznych zamiast procesorów do wykonywania operacji łamania haseł. Może to znacznie przyspieszyć proces, ponieważ procesory graficzne mogą wykonać to zadanie znacznie szybciej niż standardowe procesory.

42. A i E. Wiele nieudanych prób logowania jest pewnym znakiem, że tester penetracyjny używa narzędzia do łamania haseł metodą brute-force w celu uzyskania dostępu do systemu. Narzędzia Hydra i Medusa są w stanie przeprowadzić brutalny atak.

43. B. To wyjście zostało utworzone przez narzędzie Medusa. Medusa to narzędzie do łamania haseł metodą brute-force, które wysyła jedno hasło po drugim na dane konto użytkownika (w tym przypadku administratora) w nadziei na znalezienie właściwego.

44. B. Narzędzie CeWL można skonfigurować tak, aby przeszukiwać witrynę organizacji docelowej i gromadzić z witryny słowa kluczowe, które mogłyby być używane jako hasła przez pracowników, a następnie zapisywać je na liście. Lista może być następnie wykorzystana do przeprowadzenia ataku na hasło typu brute-force.

45. D. Narzędzie Dirbuster jest narzędziem brutalnej siły, które może być używane przez testerów penetracyjnych do wykrywania katalogów i plików na serwerze WWW lub serwerze aplikacji, w tym ukrytych plików lub katalogów.

46. C. Tęczowa tablica to wstępnie obliczona tablica wartości skrótu, której można użyć do odwrócenia funkcji skrótu. Na przykład, jeśli hasło w postaci zwykłego tekstu zostało zabezpieczone przez zaszyfrowanie, można użyć tablicy tęczowej do odwrócenia funkcji mieszania i ujawnienia oryginalnego hasła w postaci zwykłego tekstu.

47. A. Solenie haszu polega na dodaniu dodatkowych, losowych danych do operacji haszowania. Ten mechanizm jest powszechnie używany do ochrony zaszyfrowanych haseł przed odwrotnym zaszyfrowaniem (co ujawniłoby hasło w postaci zwykłego tekstu).

48. B. Rozciąganie klucza polega na wielokrotnym uruchamianiu wartości do haszowania przez funkcję haszującą. Wydłuża to czas obliczeń wymagany do zaszyfrowania każdego hasła, ale również znacznie zwiększa rozmiar tablicy tęczy potrzebnej do działania ataku z obliczeniami wstępnymi.

49. C. Nazwa użytkownika i hasło są przykładami czegoś, co znasz i dlatego nie stanowią uwierzytelniania wieloskładnikowego. Skan odcisków palców jest przykładem czegoś, czym jesteś. Wymaganie skanowania odcisków palców poprawiłoby bezpieczeństwo systemu, ponieważ do logowania użytkowników wymagane byłyby czynniki uwierzytelniające z wielu kategorii.

50. A. PIN jest przykładem czegoś, co znasz.

51. C. Dzieciakowi skryptowemu zazwyczaj brakuje zaawansowania technicznego, aby przeprowadzić atak przy użyciu własnych narzędzi. Zamiast tego zazwyczaj pobierają istniejące narzędzia i uruchamiają je. Ponieważ narzędzia te są już znane społeczności zajmującej się cyberbezpieczeństwem, skryptowe dzieciaki na ogół stanowią mniejsze zagrożenie niż inne typy aktorów na liście przeciwników.

52. D. Zaawansowane trwałe zagrożenia (APT) są często sponsorowane przez państwa narodowe, a zatem są bardzo dobrze finansowane i mają dostęp do wysokiej klasy zasobów technicznych i wiedzy. Jako taki, APT zazwyczaj stanowi największe zagrożenie ze wszystkich aktorów na liście poziomów przeciwników.

53. D. W tym scenariuszu Twoje skany zostały wykryte przez system ochrony przed włamaniami (IPS), w wyniku czego adres IP używany przez Twój laptop został umieszczony na czarnej liście. Teraz wszystkie urządzenia w sieci klienta odrzucają pakiety z adresem IP znajdującym się na czarnej liście.

54. A. Ramowa umowa o świadczenie usług (MSA) określa ogólne warunki, które będą miały zastosowanie do wielu przyszłych umów. Dlatego też umowa MSA jest zasadniczo umową, która

określa warunki, na jakich będą wykonywane przyszłe prace. Konkretne projekty regulowane przez MSA zostaną określone w oświadczeniu o pracy (SOW). Fakt, że klient chce podpisać umowę MSA, wskazuje, że prawdopodobnie chce korzystać z Twojej firmy przy wielu zleceniach.

55. B. Najprawdopodobniej klient wdrożył system kontroli dostępu do sieci (NAC). Twój laptop nie spełniał kryteriów wymaganych przez NAC, aby połączyć się z bezpieczną siecią, więc został poddany kwarantannie w odizolowanej sieci naprawczej, gdzie może uzyskać dostęp do serwera naprawczego (innego hosta w sieci), aby zapewnić zgodność.

56. C. Fakt, że administrator serwera nie odnowił swojego certyfikatu bezpieczeństwa wskazuje, że nie przywiązuje on dużej wagi do tego serwera. To uczyniłoby ten system dojrzałym celem kompromisu, ponieważ możliwe jest, że istnieją inne czynniki (takie jak aktualizacje), które administrator również pominął.

57. E. Informacje zebrane podczas skanowania podatności można podzielić na różne kategorie. Na przykład właściwe może być kategoryzacja informacji w oparciu o system operacyjny, ponieważ różne systemy operacyjne mają różne nieodłączne luki w zabezpieczeniach. Właściwe może być również kategoryzacja informacji według wartości każdego powiązanego zasobu. Na przykład luki związane z krytycznym serwerem bazy danych miałyby znacznie większą wartość niż luki związane z systemem komputerowym użytkownika końcowego. Możesz także skategoryzować wyniki skanowania na podstawie liczby lub wagi wykrytych luk w zabezpieczeniach.

58. A. Najprawdopodobniej skaner podatności wygenerował fałszywie pozytywny błąd. Celem procesu orzekania po skanowaniu luk w zabezpieczeniach jest określenie wartości i poprawności wyników skanowania. Fałszywe alarmy, takie jak te omówione w tym scenariuszu, powinny zostać odfiltrowane w końcowym raporcie dla klienta.

59. A i D. W tym scenariuszu wartość narażenia na szwank kontrolera domeny lub serwer bazy danych jest znacznie wyższy niż wartość narażenia na zagrożoną stację roboczą użytkownika końcowego. Na przykład naruszenie kontrolera domeny może ujawnić wiele kont użytkowników. Podobnie naruszenie bezpieczeństwa serwera bazy danych może ujawnić cenne informacje firmy. Z drugiej strony narażenie spowodowane brakującą aktualizacją funkcji systemu Windows jest prawdopodobnie minimalne. Podobnie Linux zapewnia stosunkowo wysoki poziom bezpieczeństwa systemu, nawet na starszej dystrybucji.

60. A. Każdy wynik CVSS mniejszy niż 4,0 jest uważany za należący do kategorii niskiego ryzyka. Dlatego wynik CVSS wynoszący 3,8 wskazuje, że jest to podatność o niskim ryzyku.

61. A. Skutecznym sposobem wykrywania luk w zabezpieczeniach związanych z określoną wersją systemu operacyjnego jest skorzystanie z bazy danych Common Vulnerabilities and Exposures (CVE). Dostęp do bazy danych CVE można uzyskać pod adresem http://cve.mitre.org. Zawiera listę publicznie znanych luk w zabezpieczeniach cybernetycznych. Za każdym razem, gdy sprzedawca odkryje lukę w swoim produkcie, dodaje wpis do bazy danych CVE. Ta baza danych zawiera informacje o lukach w zabezpieczeniach systemów operacyjnych Windows, Mac OS, Linux, UNIX, Android i iOS.

62. C i D. FTP i Telnet są uważane za niezabezpieczone usługi i protokoły. Dzieje się tak, ponieważ przesyłają dane, w tym dane uwierzytelniające, przez sieć w postaci zwykłego tekstu. Te informacje można łatwo przechwycić za pomocą sniffera pakietów.

63. A i D. Chociaż SSHv1 wykorzystuje szyfrowane transmisje danych, nie jest uważany za tak bezpieczny jak SSHv2. Jednak wiele starszych systemów Linux lub UNIX może nadal być

skonfigurowanych do korzystania z protokołu SSHv1. Podobnie TLS 1.2 jest uważany za bezpieczniejszy niż SSL 2.0.

64. B i C. Przypisanie plikowi wykonywalnemu w systemie Linux uprawnienia SUID umożliwia jego uruchomienie z uprawnieniami właściciela pliku. Jeśli właścicielem jest użytkownik root, zostanie wykonany z uprawnieniami superużytkownika roota. Podobnie, przypisanie do pliku wykonywalnego uprawnienia SGID umożliwia jego działanie z uprawnieniami grupy będącej właścicielem. Jeśli grupa będąca właścicielem jest grupą główną, to działa z uprawnieniami grupy głównej.

65. C. Gdy uprawnienie do bitów pamięci jest przypisane do katalogu w systemie Linux, użytkownicy mogą usuwać pliki tylko w katalogu, którego są właścicielami, nawet jeśli mają uprawnienia do zapisu i wykonywania w tym katalogu.

66. A. Struktura kontroli przepływu if/then w Ruby wykorzystuje następującą składnię:

```
if condition

commands...

else

commands...

end
```

67. B. Struktura kontroli przepływu if/then w PowerShell wykorzystuje następującą składnię:

```
if condition {

commands...

} Else {

commands...

}
```

68. C. Struktura kontroli przepływu if/then w Bash wykorzystuje następującą składnię:

```
if condition then

commands...

else

commands...

fi
```

69. E. Struktura sprawy jest najlepszą prezentowaną opcją do oceny dokonanego przez użytkownika wyboru wielu wyborów i uruchomienia w rezultacie odpowiedniego zestawu poleceń.

70. A. Pętla while będzie przetwarzać w kółko, dopóki określony warunek nie zmieni się na fałsz.

71. B. W tym scenariuszu pytanie mówi, że tester penetracyjny pisze raport „zakreślający ogólny poziom ryzyka”. Biorąc pod uwagę to oświadczenie, tester uwzględni te informacje w streszczeniu wykonawczym. Streszczenie to najważniejsza część raportu. Powinien być napisany w sposób, który przekazuje wszystkie ważne wnioski raportu w jasny sposób, który jest napisany „w terminach laika”.

Tester powinien wyjaśnić, co zostało odkryte prostym językiem i opisać ryzyko dla firmy w sposób zrozumiały dla klienta.

72. B. W tym scenariuszu, ponieważ tester penetracyjny wykrył krytyczną podatność, tester powinien natychmiast powiadomić klienta o szczegółach wyników.

73. A. W tym scenariuszu atakujący używał przekierowania. Analityk bezpieczeństwa powinien blokować przekierowania adresów URL. Przekierowanie adresu URL to funkcja serwera WWW, która przesyła użytkownika z jednego adresu URL do drugiego. Przekierowania zwykle przybierają formę automatycznego przekierowania, które wykorzystuje jeden z serii kodów stanu zdefiniowanych w protokole HTTP. Tak więc, gdy przeglądarka internetowa próbuje otworzyć adres URL, który ma przekierowanie, otwierana jest strona z innym adresem URL.

74. A, F i G. W tym scenariuszu tester powinien zalecić klientowi zwiększenie wymagań dotyczących złożoności haseł, ponieważ tester był w stanie je złamać za pomocą ataku słownikowego. Tester powinien również zalecić, aby wszyscy pracownicy wzięli udział w szkoleniu dotyczącym świadomości bezpieczeństwa, ponieważ to członek działu IT podał istotne informacje, gdy tester użył techniki phishingowej. Tester powinien również zalecić aktualizację szyfru pakietu używanego do rozwiązania VPN. Zestaw szyfrów to zestaw algorytmów, które pomagają zabezpieczyć połączenia sieciowe korzystające z protokołu Transport Layer Security (TLS) lub Secure Socket Layer (SSL). Zestaw algorytmów, które zwykle zawierają zestawy szyfrów, obejmuje algorytm wymiany kluczy, algorytm szyfrowania zbiorczego i algorytm kodu uwierzytelniania wiadomości (MAC).

75. A. W tym scenariuszu tester powinien zalecić klientowi włączenie HTTP Strict Transport Security (HSTS). Nagłówek odpowiedzi HSTS umożliwia witrynie internetowej poinformowanie przeglądarek, że należy uzyskać do niej dostęp tylko za pomocą protokołu HTTPS, a nie protokołu HTTP. Jest to opcjonalne rozszerzenie bezpieczeństwa, które jest określane przez aplikację internetową za pomocą specjalnego nagłówka odpowiedzi. Gdy obsługiwana przeglądarka odbierze ten nagłówek, uniemożliwi ona przesyłanie jakiejkolwiek komunikacji przez HTTP do określonej domeny i zamiast tego będzie wysyłać całą komunikację przez HTTPS.

76. B. Dostawcy usług w chmurze, tacy jak AWS, wymagają uprzedniej zgody na przeprowadzenie testu pentest w ich środowisku zewnętrznym. Ta aprobata najprawdopodobniej zostanie znaleziona w Zasadach Zaangażowania (RoE), które określają ograniczenia dotyczące wykonania pentestu.

77. C. Pytanie miało na celu zastosowanie filtra do wyników wyszukiwania konkretnie w HTTP. Standardowym portem dla ruchu HTTP jest port 80.

78. B. Port nie jest prawidłowym wyborem. Wybory, których można użyć do zastosowania filtra, można znaleźć na stronie wyników Censys po wykonaniu zapytania.

79. B. Aircrack-ng zapewnia zestaw narzędzi, które można wykorzystać do monitorowania i atakowania sieci Wi-Fi.

80. B. Karta sieci bezprzewodowej musi zostać przełączona w tryb monitorowania przed przechwytywaniem i wstrzykiwaniem pakietów do sieci. W Kali można to osiągnąć za pomocą airmon-ng start <nazwa interfejsu>.