1. D. Zasady zaangażowania zostały odpowiednio zdefiniowane w tym scenariuszu. Na przykład całkiem stosowne jest określenie, jakie zachowania obronne cel może używać podczas testu. Podobnie test białej skrzynki prawdopodobnie będzie zawierał szczegółowe informacje o sieci wewnętrznej. Nierzadko zdarza się również, że dostawcy usług zewnętrznych są wykluczani z testu.

2. A. Ponieważ jest to ocena czarnoskrzynkowa, testerzy nie powinni mieć wcześniejszej wiedzy o środowisku, które ma być testowane, ani nie powinni mieć do niego specjalnego dostępu. Zasadniczo powinni atakować klienta z tej samej perspektywy, z jakiej zrobiłby to prawdziwy napastnik. Wstrzymywanie testowania w godzinach szczytu jest całkiem właściwe, aby uniknąć zakłócenia krytycznych operacji biznesowych. Wskazane jest również, aby komunikować się z klientem dopiero po zakończeniu testu, zwłaszcza w przypadku oceny czarnej skrzynki.

3. B. Umowa testowa powinna zawierać zastrzeżenie wskazujące, że test jest ważny tylko w momencie jego przeprowadzenia oraz że zakres i metodologia wymagana przez klienta mogą mieć wpływ na kompleksowość testu. Umowa o zachowaniu poufności określa, co każda ze stron umowy może ujawnić stronom trzecim. Klauzula arbitrażowa może nadal skutkować ugodą, która jest sprzeczna z konsultantem ds. testów pisarskich. Samo SOW nie uchroni Cię przed tego rodzaju pozwem, chyba że zawiera klauzulę dotyczącą określonego momentu, o której była mowa wcześniej.

4. C. Umowa testowa lub dokumentacja zakresu powinna zawierać zastrzeżenie wyjaśniające, że zakres i metodologia wymagana przez klienta mogą wpłynąć na kompleksowość testu. Na przykład test białej skrzynki ma większe szanse na wykrycie ukrytych luk w zabezpieczeniach niż test czarnej skrzynki. Zamówienie zakupu jest wiążącą umową zakupu towarów lub usług. MSA to umowa, która określa warunki, które będą obowiązywać w przyszłych umowach. Testy czarnoskrzynkowe mogą zapewnić wyjątkową perspektywę i nie należy ich pomijać.

5. A i E. Dokumentując obsługę i rozwiązywanie problemów w dokumencie zasad zaangażowania, należy jasno zdefiniować procedury eskalacji po obu stronach umowy, aby zminimalizować przestoje w organizacji docelowej. Należy również uwzględnić słownictwo, które wymaga od klienta potwierdzenia, że testy penetracyjne niosą ze sobą nieodłączne ryzyko. Harmonogram zaangażowania wraz z informacjami o zakresie jest również zawarty w ROE, ale nie w sekcji rozwiązywania problemów.

6. D. Domyślny port używany przez usługę IMAP to 143. Protokół IMAP jest używany przez serwery pocztowe do przesyłania wiadomości między serwerem pocztowym a klientami pocztowymi.

7. C. Domyślny port używany przez usługę SSH to 22. Protokół SSH służy do zdalnego zarządzania systemami za pomocą interfejsu wiersza poleceń. W przeciwieństwie do Telnet, SSH używa szyfrowania do ochrony danych uwierzytelniających oraz danych przesyłanych między klientem a serwerem.

8. D. Domyślne porty używane przez serwer WWW to 80 (HTTP) i 443 (HTTPS). Dane przesyłane na porcie 80 są zwykle przesyłane w postaci jawnej, natomiast dane przesyłane na porcie 443 są szyfrowane przy użyciu protokołu SSL/TLS.

9. A. Domyślne porty używane przez serwer LDAP to 389 (niezabezpieczone) i 636 (zabezpieczone). Protokół LDAP służy do wysyłania zapytań do serwera katalogowego zgodnego z LDAP, takiego jak Active Directory lub eDirectory. Ponieważ informacje katalogowe wysyłane na porcie 389 nie są szyfrowane, podsłuchiwanie ruchu na tym porcie może ujawnić informacje o koncie użytkownika.

10. D. Domyślny port używany przez serwer DNS to 53. Usługa DNS służy do tłumaczenia nazw hostów na adresy IP (i odwrotnie). Jeśli serwer DNS był słabo zabezpieczony, możesz być w stanie go złamać i zatruć tabele wyszukiwania, umożliwiając przekierowywanie uzasadnionych żądań rozpoznawania

nazw do fałszywego hosta docelowego, na którym w systemach klienckich mogą być zaimplementowane różne exploity.

11. D. Tester penetracyjny wykorzystuje podobieństwo jako czynnik motywujący. Zatrudniając młodych, przyjaznych i atrakcyjnych fizycznie asystentów, tester penetracyjny jest w stanie zmusić pracowników organizacji docelowej do ujawnienia poufnych informacji o pracodawcy.

12. A. Tester penetracyjny wykorzystuje strach jako czynnik motywujący. Niezależnie od tego, czy twierdzenie jest prawdziwe, czy nie, dyrektor finansowy wie, że takie odkrycie może zaszkodzić jego rodzinie i karierze. Mogłoby to również narazić go na oskarżenie. Może to potencjalnie zmotywować go do ujawnienia poufnych informacji.

13. C. Tester penetracyjny używa autorytetu (i prawdopodobnie pilności wraz ze strachem) jako czynnika motywującego. Przedstawiciel handlowy może być skłonny utworzyć połączenie VPN, aby zapobiec rzekomej utracie ważnego klienta.

14. B. Tester penetracyjny wykorzystuje pilność (i prawdopodobnie podobieństwo) jako czynnik motywujący. Pracownik prawdopodobnie zastosuje się do prośby z chęci bycia postrzeganym jako „gracz zespołowy”. Ten rodzaj ataku może być jeszcze bardziej skuteczny, przeprowadzając wcześniej rozpoznanie i identyfikując nazwiska prawdziwych przedstawicieli handlowych pracujących dla organizacji.

15. A i B. Tester penetracyjny wykorzystuje w tym przykładzie dwa czynniki motywacyjne. Wykorzystuje pilność i dowód społeczny jako czynniki motywujące. Ponieważ jest to ogromne zamówienie, pracownik prawdopodobnie odczuwa pilną potrzebę wykonania. Tester penetracyjny wykorzystuje również dowód społeczny, wymieniając nazwisko znajomego współpracownika. Prawdopodobnie pomaga to pracownikowi poczuć się bardziej komfortowo, przekazując testerowi penetracyjnemu swoją nazwę użytkownika i hasło.

16. A. Opcja –T1 mówi nmapowi, aby skanował w trybie podstępnym. W tym trybie port będzie skanowany co 15 sekund. W związku z tym ten rodzaj skanowania jest bardzo powolny. Jednak powolność sprawia również, że skanowanie jest trudniejsze do wykrycia.

17. D. Opcja –T4 nakazuje nmapowi skanowanie w trybie agresywnym. Ten typ skanowania działa dość szybko. Szybkość sprawia jednak, że skanowanie jest łatwiejsze do wykrycia przez systemy IDS/IPS lub personel IT celu.

18. C. Jeśli polecenie nmap jest uruchamiane bez określenia opcji czasu, domyślnie używana jest opcja –T3. To mówi nmapowi, aby skanował w trybie normalnym.

19. A. Opcja –T0 powoduje, że nmap skanuje w trybie paranoidalnym, w którym co pięć minut skanowany jest tylko jeden port na hoście docelowym. Chociaż ten tryb może być używany do uruchamiania najbardziej ukrytych skanów, powoduje to również ich niezwykle powolne działanie.

20. A. Opcja –T5 powoduje, że nmap skanuje w trybie szalonym. Jest to najszybszy typ skanowania nmap. Jednak szybkość ułatwia również wykrycie przez narzędzia IDS/IPS lub personel IT celu.

21. B. Tworząc swój pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś wskazać standard lub wytyczne użyte do przeprowadzenia testu w sekcji Metodologia. W tym przykładzie poinformujesz czytelnika, że użyłeś metodologii NIST 800-115.

22. A. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, należy przedstawić ogólny opis testu oraz wyniki w streszczeniu wykonawczym. Zazwyczaj jest to pierwsza część raportu i jest przeznaczona dla mniej technicznych odbiorców.

23. D. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś zgłosić swoje oceny ryzyka w sekcji Metryki i miary. Oceny te pozwalają czytelnikowi ustalić priorytety zagrożeń, a także dokonać porównań między testami penetracyjnymi przeprowadzanymi w czasie.

24. A. Tworząc pisemny raport z ustaleń po zakończeniu testu penetracyjnego, należy przedstawić ogólny opis testu i wyniki w streszczeniu wykonawczym. Zazwyczaj jest to pierwsza część raportu i jest przeznaczona dla mniej technicznych odbiorców.

25. B. Tworząc swój pisemny raport z ustaleń po zakończeniu testu penetracyjnego, powinieneś wskazać standard lub wytyczne użyte do przeprowadzenia testu w sekcji Metodologia. W tym przykładzie poinformujesz czytelnika, że zastosowałeś metodologię CEH Rady EC.

26. E. Ponieważ w tym scenariuszu przeprowadzany jest test czarnej skrzynki, sieć klienta powinna być w trybie „shields up". Testerzy penetracji nie powinni mieć wewnętrznych kont użytkowników, a ich systemy nie powinny mieć możliwości omijania kontroli bezpieczeństwa NAC. Przypinanie certyfikatu nie powinno być dozwolone.

27. A. Normalnie, gdy NAC jest wdrażany z IPSec, klienci muszą spełniać firmowe zasady bezpieczeństwa, zanim będą mogli połączyć się z wewnętrzną bezpieczną siecią. Jeśli tak, otrzymują certyfikat cyfrowy, który pozwala im komunikować się z innymi systemami w bezpiecznej sieci wewnętrznej. Aby ominąć NAC, można użyć przypinania certyfikatów do przypisania certyfikatu cyfrowego do systemów testerów bez udowadniania ich zgodności przy każdym połączeniu.

28. A. To jest przykład unikania ryzyka. Dzięki usunięciu drzwi i wypełnieniu ściany betonem, klient całkowicie wyeliminował ryzyko wykorzystania drzwi przez napastnika w celu uzyskania nieautoryzowanego dostępu do obiektu.

29. C. To jest przykład ograniczania ryzyka. Zamiast całkowicie usunąć ryzyko, klient zastosował ochroniarza jako środek zaradczy. Ryzyko nieautoryzowanego dostępu nadal istnieje, ale użycie ochroniarza kontroluje to ryzyko.

30. B. To jest przykład przeniesienia ryzyka. Zamiast unikać ryzyka lub je ograniczać, klient przeniósł ryzyko na podmiot zewnętrzny.

31. A. Skanowanie w poszukiwaniu poświadczonych luk w zabezpieczeniach wymaga uprzedniego uwierzytelnienia w sieci, najlepiej za pomocą konta na poziomie administracyjnym. Ponieważ używane są poświadczenia administracyjne, ten typ skanowania jest najbardziej zbliżony do perspektywy administratora wewnętrznego.

32. B. Skanowanie luk w zabezpieczeniach bez uwierzytelnienia jest wykonywane bez uwierzytelniania w sieci. Z tego powodu skan bez uwierzytelnienia najbardziej przypomina perspektywę zewnętrznego hakera.

33. A. Skanowanie w poszukiwaniu poświadczonych luk w zabezpieczeniach wymaga uprzedniego uwierzytelnienia w sieci, najlepiej za pomocą konta na poziomie administracyjnym. Ponieważ używane są poświadczenia administracyjne, ten typ skanowania zwykle identyfikuje najwięcej luk.

34. B. Skanowanie podatności bez danych uwierzytelniających jest wykonywane bez uwierzytelniania w sieci. Z tego powodu skanowanie bez poświadczeń zwykle identyfikuje najmniejszą liczbę luk w zabezpieczeniach.

35. A. Przykładem skanowania odnajdującego jest ping sweep. Celem przeszukiwania ping nie jest przesłuchiwanie każdego systemu. Zamiast tego po prostu stara się zidentyfikować obecność każdego osiągalnego systemu w sieci.

36. B. Atak typu ARP spoofing jest klasyfikowany jako atak typu man-in-the-middle.

37. D. To jest przykład ponownego ataku. Tester przechwytuje prawidłowe dane uzgadniania z sieci bezprzewodowej i odtwarza je później, aby uwierzytelnić swój laptop w sieci bezprzewodowej.

38. D. Atak powtórkowy jest również klasyfikowany jako atak typu man-in-the-middle.

39. A. To jest przykład ataku sztafetowego. Atakujący siedzi pomiędzy dwoma hostami komunikującymi się w sieci, w tym przypadku stacją roboczą i serwerem. Dla serwera atakujący podszywa się pod stację roboczą. Na stacji roboczej atakujący podszywa się pod serwer.

40. A. Jest to również przykład ataku sztafetowego. Atakujący siedzi pomiędzy dwoma hostami komunikującymi się w sieci, w tym przypadku stacją roboczą i serwerem. Dla serwera atakujący podszywa się pod stację roboczą. Na stacji roboczej atakujący podszywa się pod serwer. W ataku przekaźnikowym człowiek w środku może, ale nie musi, modyfikować dane przesyłane między dwoma hostami.

41. A. To dzieło zostało stworzone przez Jana Rozpruwacza. To narzędzie do testowania poświadczeń jest narzędziem do łamania haseł typu bruteforce. W tym przykładzie wykryto hasło użytkownika root (toor).

42. A. Dane wyjściowe zostały utworzone przez narzędzie whois. To narzędzie OSINT służy do zbierania publicznych informacji o domenie organizacji docelowej.

43. D i E. Możesz użyć Kismet lub WiFite, aby spróbować złamać sieć bezprzewodową organizacji docelowej. Możesz również użyć Aircrack-ng, aby to osiągnąć.

44. B i C. Możesz użyć Burp Suite lub OWASP ZAP. Oba te narzędzia można wykorzystać do przechwytywania ruchu sieciowego przepływającego między użytkownikami korzystającymi z przeglądarki internetowej a serwerem aplikacji internetowych docelowej organizacji. Poprzez proxy połączenia, tester penetracyjny może odczytać zawartość przechwyconego ruchu.

45. A. Narzędzie netcat może być użyte do skonfigurowania exploita odwróconej powłoki, który umożliwia testerowi zdalne kontrolowanie zaatakowanego systemu.

46. C. Skan siatkówki jest przykładem czegoś, czym jesteś. Teoretycznie żadne dwie osoby nie powinny mieć identycznych atrybutów dla tego typu czynnika.

47. C. Połączenie przewodowe z wewnętrzną siecią LAN organizacji jest przykładem miejsca, w którym jesteś. Uwierzytelnianie może, ale nie musi być dozwolone na podstawie tego czynnika.

48. A. Czytnik zbliżeniowy RFID może być użyty, aby uniemożliwić użytkownikowi uwierzytelnianie w systemie, chyba że są one fizycznie obecne w systemie.

49. C. Wymaganie od użytkownika dostarczenia skanu biometrycznego (coś, czym jesteś) wraz z kodem PIN (coś, co znasz) stanowi uwierzytelnianie wieloskładnikowe.

50. B. Wymaganie od użytkownika podania hasła (coś, co znasz) oraz generatora tokenów bezpieczeństwa (coś, co masz) stanowi uwierzytelnianie wieloskładnikowe.

51. E. W tym scenariuszu przeprowadzany jest test penetracyjny zespołu czerwonego. Ocena zespołu czerwonego zwykle ma wąskie cele, zamiast próbować kompleksowo zidentyfikować i przetestować wszystkie możliwe luki. Czerwona ocena zespołu może wykorzystywać skoordynowany atak pochodzący z wielu różnych wektorów, aby osiągnąć te cele. Aby to osiągnąć, zespół może korzystać z szerokiej gamy narzędzi i technik, w tym z technologicznych, fizycznych i społecznych nadużyć.

52. D. Wiedza o tym, które identyfikatory SSID są objęte zakresem, ma kluczowe znaczenie podczas przeprowadzania testu penetracyjnego w obiekcie współdzielonym z wieloma najemcami. Naruszenie niewłaściwej sieci bezprzewodowej jest nielegalne i może skutkować wniesieniem oskarżenia i/lub pozwem sądowym.

53. A i D. Podmioty zajmujące się przestępczością zorganizowaną i zagrożeniami państwowymi zazwyczaj mają dostęp do rozległych zasobów finansowych i wiedzy technicznej. To wiele razy pozwala im tworzyć własne, niestandardowe exploity, które nie są używane przez nikogo innego.

54. B. Złośliwy insider to zazwyczaj pracownik lub kontrahent, któremu zgodnie z prawem przyznano dostęp do informacji i systemów organizacji. Złośliwy insider wykorzystuje to zaufanie i wykorzystuje je do złamania zabezpieczeń informacji lub systemów organizacji.

55. 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.

56. D. Każdy wynik CVSS wynoszący 10,0 lub wyższy jest uważany za należący do kategorii ryzyka krytycznego. Dlatego wynik CVSS równy 10 wskazuje, że jest to krytyczna podatność.

57. B. Każdy wynik CVSS pomiędzy 4,0 a 6,0 jest uważany za należący do kategorii średniego ryzyka. Dlatego wynik CVSS wynoszący 5,3 wskazuje, że jest to podatność na średnie ryzyko.

58. C. Każdy wynik CVSS pomiędzy 6,0 a 10,0 jest uważany za należący do kategorii wysokiego ryzyka. Dlatego wynik CVSS wynoszący 7,2 wskazuje, że jest to podatność na wysokie ryzyko.

59. B i C. Twoją pierwszą odpowiedzią na powszechny temat brakujących aktualizacji byłoby zbadanie, czy tworzy to jakiekolwiek luki, które mógłbyś wykorzystać później w teście penetracyjnym. Następnie należy udokumentować wspólny motyw brakujących aktualizacji, aby klient mógł zaktualizować swoje najlepsze praktyki, aby zapewnić aktualność systemów.

60. A. Pierwszą reakcją na twoją obserwację przestarzałych serwerów byłoby zbadanie, czy stwarza to jakiekolwiek luki, które mógłbyś wykorzystać później w teście penetracyjnym. Następnie powinieneś zalecić klientowi aktualizację serwera w raporcie końcowym.

61. A. W systemie Linux standardowy użytkownik może uruchomić plik wykonywalny za pomocą programu sudo w celu podniesienia uprawnień i uruchomić plik wykonywalny jako użytkownik root (lub dowolny inny użytkownik w systemie, jeśli to konieczne).

62. C. W systemie Linux exploit Ret2libc powoduje zastąpienie adresu zwrotnego podprogramu adresem podprogramu, który jest już obecny w pamięci procesu.

63. A. W systemie Windows cPassword jest nazwą atrybutu przechowującego hasła w elemencie Preferencje zasad grupy. Za każdym razem, gdy preferencja wymaga zapisania hasła użytkownika, jest

ono przechowywane w tym atrybucie w zaszyfrowanym formacie. Hasło może jednak łatwo odszyfrować każdy uwierzytelniony użytkownik w domenie.

64. B. Zaleca się używanie LDAPS na porcie 636 do zarządzania kontami użytkowników. LDAPS jest zabezpieczony SSL. Standardowy protokół LDAP na porcie 389 przesyła dane w sieci w postaci zwykłego tekstu. Oznacza to, że poświadczenia użytkownika administracyjnego, które przesyłasz w celu uzyskania dostępu do samej usługi katalogowej, a także wszelkie poświadczenia zarządzanych użytkowników są przesyłane w postaci zwykłego tekstu.

65. B. Tester penetracji w tym scenariuszu używa exploita Kerberoasting. Każdy prawidłowy użytkownik domeny może zażądać nazwy SPN dla zarejestrowanej usługi. Otrzymany w rezultacie bilet Kerberos może zostać przeniesiony do trybu offline i złamany, co może potencjalnie ujawnić hasło do konta usługi. Może to umożliwić eskalację uprawnień, ponieważ nierzadko konto usługi ma uprawnienia administratora do serwera lokalnego.

66. D. Struktura if/then/else jest uważana za strukturę kontroli przepływu, ponieważ rozgałęzia skrypt w jednym z kilku kierunków w oparciu o sposób oceny określonego warunku.

67. C. Struktura pętli until będzie kontynuować przetwarzanie tak długo, jak określony warunek będzie miał wartość false.

68. B. Struktura pętli for będzie przetwarzać określoną liczbę razy.

69. D. Dodanie linii $TargetHost = read-host -Prompt do skryptu PowerShell powoduje, że akceptuje on dane wejściowe wprowadzone w wierszu poleceń przez użytkownika i przypisuje je do zmiennej o nazwie TargetHost.

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

71. C. W tym scenariuszu ważne byłoby umieszczenie tolerancji ryzyka organizacji klienta w streszczeniu wykonawczym. Tolerancja na ryzyko to w zasadzie to, jak duże ryzyko organizacja jest gotowa podjąć, jeśli chodzi o jej inwestycje. W przypadku każdego rodzaju inwestycji zawsze istnieje ryzyko, ale to, ile ryzyka można wytrzymać, to ich tolerancja na ryzyko. To może być inne dla każdej organizacji. Nie można ustalić ustalonej wartości tolerancji ryzyka.

72. D. W tym scenariuszu, ponieważ testy zostały przeprowadzone przez młodszego administratora na stanowisku, w najlepszym interesie firmy może być utworzenie zapytania ofertowego (RFP) od profesjonalnej firmy zajmującej się testami penetracyjnymi w celu uzgodnienia ocen i aby przekazać firmie wszelkie ustalenia dotyczące luk w zabezpieczeniach. Zapytanie ofertowe to dokument, w którym pozyskuje się propozycję, często składaną w ramach procedury przetargowej.

73. A. W tym scenariuszu pyta, co analityk bezpieczeństwa powinien zrobić w pierwszej kolejności. Po zidentyfikowaniu luki należy ocenić ryzyko i sposób, w jaki wpływa ono na Twoją organizację. Ocena określi, czy kontynuowanie pracy jest wystarczająco bezpieczne, czy też konieczne jest podjęcie dodatkowych środków kontroli w celu zmniejszenia lub wyeliminowania ryzyka. Ocena zależy od prawdopodobieństwa wystąpienia zdarzenia i wagi luk. Odbywa się to poprzez ustalenie, czy prawdopodobieństwo jest niskie, średnie czy wysokie i następnie robi to samo dla wpływu. Skala od 0 do 9 jest podzielona na trzy części: od 0 do < 3 to Niska, od 3 do < 6 to Średnia, a od 6 do 9 to Wysoka.

74. A. W tym scenariuszu najlepiej byłoby ponownie przyjrzeć się tej sytuacji na etapie wyciągania wniosków. Sesja wyciągnięta z wniosków jest okazją zespołu do zebrania się i omówienia procesu testowania i wyników bez obecności klienta. Członkowie zespołu powinni swobodnie omawiać test i

przedstawiać sugestie dotyczące ulepszeń. Sesja wyciągnięta z wyciągniętych wniosków jest dobrą okazją do podkreślenia wszelkich innowacyjnych technik użytych podczas testu, które mogą być wykorzystane w przyszłych zobowiązaniach.

75. B. W tym scenariuszu najlepszą opcją poinformowania klienta byłoby użycie kart inteligentnych i kodów PIN. Uwierzytelnianie wieloskładnikowe (MFA) to system zabezpieczeń, który wymaga więcej niż jednej metody uwierzytelniania z oddzielnych kategorii poświadczeń, aby zweryfikować tożsamość użytkownika podczas logowania lub innej transakcji. Kategorie uwierzytelniania to coś, co znasz, coś, co masz i coś, czym jesteś.

76. A. Ramy zarządzania umożliwiają stacjom lub klientom utrzymanie komunikacji z AP i obejmuje wiele podtypów, w tym poświadczenie.

77. A. Ramka sygnału nawigacyjnego zawiera ważne informacje o połączeniu i asocjacji z innymi stacjami/klientami z AP.

78. D. Wszystkie RTOS muszą przestrzegać ograniczeń czasowych, niezależnie od wpływu.

79. A. Prawidłowa odpowiedź to OWASP ZAP.

80. C. Poprawną odpowiedzią jest plik robots.txt.