1. B. Etap rekonesansu map Cyber Kill Chain do gromadzenia informacji i identyfikacja podatności na etapie procesu testowania penetracyjnego. Pozostałe sześć etapów Cyber Kill Chain to mapa do fazy Ataku i Wyzysku w procesie testowania penetracji.

2. B. Podczas gdy Robert rzeczywiście zbiera informacje podczas ataku phishingowego, przeprowadza aktywny atak socjotechniczny. Wykracza to poza działania związane z gromadzeniem informacji i identyfikacją podatności i przenosi się w sferę atakowania i wykorzystywania.

3. C. Nmap to narzędzie do skanowania portów używane do wyliczania otwartych portów sieciowych w systemie. Nessus to skaner podatności zaprojektowany do wykrywania problemów z bezpieczeństwem w systemie. Nslookup to narzędzie do zbierania informacji DNS. Wszystkie trzy z tych narzędzi mogą służyć do zbierania informacji i wykrywania luk w zabezpieczeniach. Metasploit to platforma eksploatacyjna służąca do wykonywania i atakowania, która lepiej nadaje się do fazy atakowania i wykorzystywania w teście penetracyjnym.

4. C. Atakujący realizuje swoje pierwotne zamiary naruszenia poufności, integralność i/lub dostępność informacji lub systemów na etapie działań dotyczących celów łańcucha cyberzabójstw.

5. C. Rozpowszechnianie zainfekowanych nośników (lub pozostawianie ich w miejscu, w którym można je znaleźć) jest przykładem fazy dostarczania łańcucha cyberzabójstw. Proces przechodzi od dostarczania do instalacji, jeśli użytkownik uruchomi złośliwe oprogramowanie na urządzeniu.

6. C. Whois i Nslookup to narzędzia służące do zbierania informacji o domenach i adresach IP. Foca służy do zbierania informacji z plików. Wszystkie trzy z tych narzędzi to narzędzia OSINT. Nessus to komercyjny skaner luk w zabezpieczeniach.

7. A. Metasploit to najpopularniejszy framework do eksploatacji wykorzystywany przez testerów penetracyjnych. Wireshark to analizator protokołów. Aircrack-ng to narzędzie do testowania bezpieczeństwa sieci bezprzewodowej. Zestaw narzędzi inżyniera społecznego (SET) to platforma do przeprowadzania ataków socjotechnicznych.

8. A. Master Services Agreement (MSA) to umowa, która określa warunki, na jakich będą wykonywane przyszłe prace. Konkretna praca jest wtedy zwykle wykonywana na podstawie oświadczenia o pracy lub SOW.

9. C. Organizacja, którą testuje Robert, prawdopodobnie wdrożyła kontrolę dostępu do sieci (NAC). Jego system nie będzie miał zainstalowanego odpowiedniego klienta NAC i nie będzie mógł uzyskać dostępu do tego gniazda sieciowego bez uwierzytelnienia i zatwierdzenia systemu przez system NAC.

10. D. Ocena czerwonej drużyny ma na celu symulację rzeczywistego ataku lub penetracji, a testerzy skupią się na znalezieniu sposobów i maksymalizacji dostępu, a nie na kompleksowej identyfikacji i testowaniu wszystkich luk i usterek, które mogą znaleźć.

11. C. Znajomość identyfikatorów SSID, które są objęte zakresem, ma kluczowe znaczenie podczas pracy we wspólnych budynkach. Penetracja niewłaściwej sieci może spowodować reperkusje prawne, a nawet karne dla nieostrożnego testera penetracyjnego!

12. B. Dzieciaki skryptowe najprawdopodobniej używają tylko gotowych narzędzi i technik ataku. Bardziej zaawansowane zagrożenia dostosują istniejące narzędzia, a nawet zbudują zupełnie nowe narzędzia i techniki, aby złamać cel.

13. C. Pełzanie zakresu występuje, gdy do zakresu oceny dodawane są dodatkowe elementy. Robert wyszedł poza zakres umowy o wstępnej ocenie. Może to być kosztowne dla klientów lub może

kosztować Roberta dochód, jeśli dodatkowy czas i wysiłek nie zostaną uwzględnione w aneksie do jego istniejącej umowy.

14. D. Standard PCI DSS to branżowy standard zgodności dla organizacji przetwarzających karty kredytowe. Dlatego Robert przeprowadza ocenę zgodności.

15. D. Pełny zakres portów dostępnych dla usług TCP i UDP to 1–65 535. Chociaż port 0 istnieje, jest portem zarezerwowanym i nie należy go używać.

16. D. Skanowanie połączenia TCP (-sT) jest często używane, gdy jedyną opcją testera jest konto nieuprzywilejowane. Systemy Linux zazwyczaj nie pozwalają kontu nieuprzywilejowanemu na bezpośredni dostęp do tworzenia pakietów, ale umożliwiają kontom wysyłanie ruchu. Robert prawdopodobnie nie będzie mógł użyć skanowania TCP SYN, ale skanowanie połączenia prawdopodobnie zadziała. Pozostałe pokazane flagi służą do testowania wersji (-sV) i wyboru typu wyjścia (-oA), a -u w ogóle nic nie robi.

17. C. Whois dostarcza informacje, które mogą obejmować adres fizyczny organizacji, rejestratora, dane kontaktowe i inne szczegóły. Nslookup dostarczy informacje o adresie IP lub nazwie hosta, podczas gdy Host zapewni adresy IPv4 i IPv6, a także informacje o usługach e-mail. Traceroute próbuje zidentyfikować ścieżkę do zdalnego hosta oraz systemy na trasie.

18. C. Flaga -T w Nmap jest używana do ustawiania czasu skanowania. Ustawienia czasu wahają się od 0 (paranoidalny) do 5 (szalony). Domyślnie działa na 3, czyli normalnie. Z czasem ustawionym na bardzo małą prędkość, skanowanie będzie postępować powoli, a Robertowi zajmie bardzo, bardzo dużo czasu, aby ukończyć skanowanie w sieci /16.

19. B. Format wyjściowy Script Kiddie obsługiwany przez Nmapa jest całkowicie dla zabawy -nigdy nie powinieneś mieć praktycznej potrzeby używania flagi -oS do rzeczywistego testu penetracji.

20. B. Polecenie strings analizuje plik pod kątem łańcuchów tekstu i wyświetla je. Często jest przydatny do analizowania plików binarnych, ponieważ możesz szybko sprawdzić przydatne informacje za pomocą jednego szybkiego narzędzia wiersza poleceń. NETCAT, choć często nazywany szwajcarskim nożem wojskowym testera, nie jest przydatny do tego typu analiz. Eclipse jest środowiskiem IDE i w niektórych przypadkach przyda się do edycji kodu lub zarządzania pełnym dekompilatorem.

21. D. Skanowania z poświadczeniami wymagają dostępu tylko do odczytu do serwerów docelowych. Renee powinna przestrzegać zasady najmniejszych uprawnień i ograniczyć dostęp do skanera.

22. C. Common Product Enumeration (CPE) to składnik SCAP, który zapewnia ustandaryzowaną nomenklaturę nazw i wersji produktów. 23. D. Ponieważ jest to skanowanie czarnoskrzynkowe, Robert nie powinien (i najprawdopodobniej nie może) przeprowadzać skanowania wewnętrznego, dopóki najpierw nie zhakuje hosta wewnętrznego. Gdy zdobędzie ten przyczółek w sieci, może użyć tego skompromitowanego systemu jako punktu startowego do wewnętrznych skanów.

24. C. Ustawa o Federalnym Zarządzaniu Bezpieczeństwem Informacji (FISMA) wymaga, aby agencje rządowe przeprowadzały skanowanie podatności. HIPAA, który reguluje szpitale i gabinety lekarskie, nie zawiera wymogu skanowania podatności, podobnie jak GLBA, która obejmuje instytucje finansowe.

25. C. Urządzenia Internetu rzeczy (IoT) są przykładami nietradycyjnych systemów, które mogą być delikatne i bardzo podatne na awarie podczas skanowania luk w zabezpieczeniach. Serwery internetowe i zapory są zazwyczaj projektowane z myślą o wystawieniu na działanie szerszych sieci i są mniej podatne na awarie podczas skanowania.

26. B. Apetyt organizacji na ryzyko to chęć tolerowania ryzyka w środowisku. Jeśli organizacja jest wyjątkowo niechętna ryzyku, może zdecydować się na częstsze skanowanie, aby zminimalizować czas między pojawieniem się luki w zabezpieczeniach a jej wykryciem przez skanowanie.

27. D. Harmonogramy skanowania są najczęściej określane przez apetyt na ryzyko organizacji, wymagania regulacyjne, ograniczenia techniczne, ograniczenia biznesowe i ograniczenia licencyjne. Większość skanów jest zautomatyzowana i nie wymaga dostępności personelu.

28. A. Błąd fałszywie pozytywny występuje, gdy skaner luk w zabezpieczeniach zgłasza lukę, która w rzeczywistości nie istnieje.

29. B. Jest mało prawdopodobne, aby tabela bazy danych zawierała informacje istotne dla oceny raportu skanowania podatności. Dzienniki, raporty SIEM i systemy zarządzania konfiguracją znacznie częściej zawierają istotne informacje.

30. O. Firma Microsoft zakończyła wsparcie dla systemu Windows Server 2003 i prawdopodobnie system operacyjny zawiera luki w zabezpieczeniach, których nie można naprawić.

31. D. Ataki przepełnienia bufora występują, gdy atakujący manipuluje programem w celu umieszczenia większej ilości danych w obszarze pamięci niż jest przydzielone do użytku tego programu. Celem jest nadpisanie innych informacji w pamięci instrukcjami, które mogą zostać wykonane przez inny proces działający w systemie.

32. B. W październiku 2016 analitycy bezpieczeństwa ogłosili odkrycie luki w jądrze Linuksa o nazwie Dirty COW. Ta luka, obecna w jądrze Linuksa od dziewięciu lat, była niezwykle łatwa do wykorzystania i zapewniała skutecznym atakującym kontrolę administracyjną nad systemami, których dotyczy problem, określaną również jako eskalacja uprawnień.

33. D. Telnet to niezabezpieczony protokół, który nie wykorzystuje szyfrowania. Wszystkie pozostałe wymienione protokoły są uważane za bezpieczne.

34. C. Meterpreter to narzędzie rezydujące w pamięci, które wstrzykuje się do innego procesu. Najbardziej prawdopodobną odpowiedzią jest to, że system został ponownie uruchomiony, usuwając w ten sposób rezydujący w pamięci proces Meterpretera. Robert może po prostu powtórzyć swój exploit, aby odzyskać dostęp, ale może chcieć podjąć dodatkowe kroki, aby zapewnić ciągły dostęp.

35. D. John the Ripper zawiera automatyczne wykrywanie typu skrótu, więc Robert może po prostu podać mu plik z haszowanym hasłem. Jeśli jest w formacie, który rozpoznaje John the Ripper, spróbuje złamać hasła. Żadna z pozostałych opcji nie jest potrzebna.

36. C. Kod kompilacji krzyżowej jest używany, gdy platforma docelowa działa w innej architekturze. Robert może nie mieć dostępu do kompilatora na swojej maszynie docelowej lub musi skompilować kod exploita ze swojej podstawowej stacji roboczej, która nie ma tej samej architektury, co jego cel.

37. B. Robert może chcieć spróbować słownikowego ataku brute-force w celu sprawdzenia słabych haseł. Powinien stworzyć niestandardowy słownik dla swojej organizacji docelowej i może chcieć wcześniej wykonać pewne prace związane z socjotechniką lub ocenić media społecznościowe, aby pomóc mu zidentyfikować wszelkie typowe zachowania związane z wyborem haseł, które mają tendencję do wyświetlania członkowie organizacji.

38. C. PSRemote lub PowerShell Remote zapewnia dostęp do wiersza poleceń z systemów zdalnych. Po ustanowieniu zdalnej relacji zaufania przy użyciu prawidłowych poświadczeń można używać poleceń programu PowerShell do różnych działań związanych z wykorzystywaniem i gromadzeniem

informacji, w tym za pomocą dedykowanych narzędzi do wykorzystywania zasobów programu PowerShell.

39. A. Harmonogram zadań systemu Windows jest używany do zaplanowanych zadań. W systemie Linux zadania cron są ustawione tak, aby uruchamiać aplikacje i inne zdarzenia na czas. Inne popularne sposoby tworzenia trwałego dostępu do systemów Linux obejmują modyfikowanie demonów systemowych, zastępowanie usług wersjami trojanów, a nawet tworzenie kont użytkowników do późniejszego wykorzystania.

40. D. Metasploit musi znać zdalny host docelowy, znany jako rhost, a ten nie został ustawiony. Tim może to ustawić wpisując set rhost [adres ip] z właściwym adresem IP. Niektóre ładunki wymagają również ustawienia lhost lub hosta lokalnego, co sprawia, że dobrym pomysłem jest użycie polecenia show options przed uruchomieniem exploita.

41. D. Ataki typu downgrade działają, powodując, że klient i serwer lub punkt dostępowy negocjują użycie mniej bezpiecznego protokołu. Może to pozwolić atakującemu na łatwiejsze złamanie szyfrowania lub innych mechanizmów ochrony używanych do zabezpieczania ruchu.

42. B. Hydra używa domyślnie 16 równoległych zadań na cel, ale można to zmienić za pomocą flagi -t.

43. FTP jest protokołem nieszyfrowanym, co oznacza, że Robert może po prostu przechwycić ruch FTP przy następnym logowaniu użytkownika do serwera FTP z systemu docelowego. Atak brute-force może się powieść, ale jest bardziej prawdopodobne, że zostanie zauważony. Chociaż może istnieć exploit, pytanie o nim nie wspomina, a nawet jeśli istnieje, niekoniecznie zapewni dane uwierzytelniające. Wreszcie, ataki typu downgrade nie są przydatne w przypadku serwerów FTP.

44. B. VRFY sprawdza, czy adres istnieje, podczas gdy EXPN pyta o członkostwo na liście mailingowej. Oba mogą być używane do weryfikacji identyfikatorów użytkowników.

45. D. Domyślny ciąg społeczności tylko do odczytu dla wielu urządzeń jest ustawiony na public. Typową najlepszą praktyką jest zmiana wszystkich ciągów społeczności na urządzeniach, aby zapobiec ich wysyłaniu bez pozwolenia.

46. B. W przeciwieństwie do innych wymienionych tutaj opcji, Mimikatz pobiera skróty z procesu lsass. Ponieważ pytanie wyraźnie mówi „przez drut”, Mimikatz jest jedynym narzędziem, którego nie można do tego użyć.

47. C. Wszystkie te narzędzia są narzędziami typu „odmowa usługi” (DoS). Chociaż niektóre z nich zostały wykorzystane do ataków DDoS, same w sobie nie są narzędziami DDoS.

48. B. Robert przeprowadza atak typu spear phishing. Ataki typu spear phishing są wymierzone w określone osoby. Jeśli Robert celował w grupę ważnych osób, może to być atak wielorybniczy. Na to pytanie wymyślono przynęty na CEO, phish hooking i Hook SETting.

49. A. Robert powinien zauważyć obecność czujnika wyjścia. Jeśli może wrócić po godzinach i spowodować, że czujnik wyskoczy zza drzwi, prawdopodobnie uzyska dostęp do centrum danych.

50. D. Robert może spróbować nurkowania w śmietniku. Kosz organizacji może być skarbnicą informacji o organizacji, jej pracownikach i bieżącej działalności na podstawie wyrzucanych dokumentów i plików. Może nawet odkryć całe komputery lub wyrzucone nośniki!

51. B. Legalność wytrychów różni się w zależności od stanu w USA. Chociaż są one legalne w większości stanów, przed podróżą Robert powinien sprawdzić legalność wytrychów w stanie docelowym i we wszystkich stanach, przez które będzie podróżował.

52. C. Dowód społeczny polega na przekonywaniu jednostki, że może zachowywać się w sposób podobny do tego, w jaki sądzą, że zachowują się inni. Scenariusz dowodu społecznego może obejmować wyjaśnienie adresatowi, że udostępnianie haseł jest powszechnie stosowane wśród pracowników w określonych okolicznościach lub że powszechną praktyką jest wpuszczanie innych pracowników przez bezpieczne drzwi bez identyfikatora.

53. D. Domyślny ciąg społeczności tylko do odczytu dla wielu urządzeń jest ustawiony na „public". Typową najlepszą praktyką jest zmiana wszystkich ciągów społeczności na urządzeniach, aby zapobiec ich wysyłaniu bez pozwolenia.

54. B. Organizacje często próbują zmniejszyć prawdopodobieństwo przeskoczenia ogrodzenia, instalując drut kolczasty, zwiększając wysokość ogrodzenia i używając ochroniarzy lub psów stróżujących. Brama nie zmniejsza prawdopodobieństwa przeskoczenia ogrodzenia i może zapewnić wejście dobremu inżynierowi społecznemu, który nie chce wspinać się po wysokim ogrodzeniu z drutem kolczastym, gdy goni go pies stróżujący.

55. D. Niezweryfikowane przekierowania instruują aplikację internetową, aby kierowała użytkowników do dowolnej witryny po zakończeniu transakcji. Takie podejście jest dość niebezpieczne, ponieważ umożliwia atakującemu wysyłanie użytkowników do złośliwej witryny za pośrednictwem legalnej witryny, której ufają. Robert powinien ograniczyć przekierowania, aby występowały tylko w jego zaufanych domenach.

56. C. Ten ciąg zapytania wskazuje na atak zanieczyszczenia parametrów. W tym przypadku wydaje się, że atakujący przeprowadzał atak typu SQL injection i próbował użyć zanieczyszczenia parametrów, aby przesunąć atak poza technologię filtrowania treści. Dwa wystąpienia serviceIDparameter w ciągu zapytania wskazują próbę zanieczyszczenia parametrów.

57. A. Seria tysięcy żądań zwiększających wartość zmiennej wskazuje, że osoba atakująca najprawdopodobniej próbowała wykorzystać niezabezpieczoną lukę w zabezpieczeniach bezpośredniego odwołania do obiektu.

58. C. W tym przypadku operatory .. są wskazówką, że atakujący próbował przeprowadzić atak z przechodzeniem katalogu. Ten konkretny atak miał na celu wyrwanie się z katalogu głównego serwera WWW i uzyskanie dostępu do pliku /etc/passwd na serwerze.

59. C. Ataki typu cross-site request forgery (XSRF) działają poprzez uzasadnione założenie, że użytkownicy często są zalogowani na wielu różnych stronach jednocześnie. Atakujący następnie umieszczają kod w jednej witrynie, który wysyła polecenie do drugiej witryny.

60. D. Ataki XSS oparte na DOM ukrywają kod ataku w Document Object Model. Ten kod nie byłby widoczny dla osoby przeglądającej źródło HTML strony. Inne ataki XSS pozostawiłyby widoczne ślady w przeglądarce.

61. B. Lokalizacja rejestru sekretów LSA w systemach Windows znajduje się pod adresem HKEY_LOCAL_MACHINE/Security/Policy/Secrets. Zawiera hasło zalogowanego użytkownika w postaci zaszyfrowanej, ale hasło jest przechowywane w kluczu Policy.

62. C. Włączenie WDigest w nowoczesnym systemie Windows, który już został skompromitowany, spowoduje, że będzie on buforował hasła w postaci zwykłego tekstu, gdy każdy użytkownik zaloguje się jako następny.

63. B. Robert powinien szukać usługi działającej jako system, aby odnieść największy sukces. Root nie jest powszechnie używaną nazwą użytkownika w systemie Windows, konta użytkowników

zaawansowanych zazwyczaj nie będą miały takiego samego dostępu, jak system, a własne konto usługi będzie często bardzo ograniczone.

64. B. Pierwszym krokiem w ataku Kerberoasting jest skanowanie kont Active Directory z ustawionymi nazwami głównymi usługi (SPN). Następnie powinien zażądać biletów serwisowych przy użyciu nazw SPN, a następnie wyodrębnić bilety serwisowe. Po otrzymaniu biletów może przeprowadzić na nie atak brute-force w trybie offline, aby odzyskać hasła używane do zaszyfrowania biletów.

65. C. Ta sytuacja wymaga narzędzia, które skutecznie radzi sobie z atakami na wiele maszyn. Na szczęście Hydra jest przeznaczona właśnie do tego i zawiera obsługę skrótów NTLM jako hasła — w rzeczywistości Medusa też to robi. Hashcat to narzędzie do łamania i odzyskiwania haseł, podczas gdy smbclient jest legalnym narzędziem klienckim SMB i nie jest przeznaczony do przeprowadzania testów w całej sieci pod kątem możliwości wykorzystania funkcji pass-the-hash.

66. B. Keyloggery sprzętowe mogą zostać wykryte, co skutkuje niepowodzeniem testu penetracyjnego. Na szczęście dla testerów penetracji, starannie umieszczone lub zakamuflowane fizyczne keyloggery z większym prawdopodobieństwem pozostaną niezauważone w wielu środowiskach. Nie są znane z awarii sprzętu, a większość z nich albo przestanie rejestrować naciśnięcia klawiszy, albo nadpisze istniejące dane, gdy są pełne. Wykrywanie keyloggerów za pomocą oprogramowania jest trudne, ponieważ często są one zamaskowane jako klawiatury lub inne typowe urządzenia, co utrudnia administratorom ich odnalezienie w dziennikach urządzeń.

67. B. Porty debugowania JTAG mogą zapewnić lepszą widoczność ściśle zintegrowanych rozwiązań sprzętowych i programowych, w tym możliwość bezpośredniego dostępu do pamięci. Może to zapewnić dostęp do kluczy szyfrowania, haseł lub innych możliwości, do których dostęp w innym przypadku byłby utrudniony dla testerów penetracyjnych. Dostęp JTAG jest na poziomie oprogramowania układowego, a nie jako zalogowany użytkownik i nie zapewnia zdalnego dostępu ani logowania.

68. C. Operator == sprawdza równość w Ruby i Pythonie, podczas gdy operator != sprawdza nierówność w tych językach. Operator -eq sprawdza równość w Bash i PowerShell, podczas gdy operator -ne sprawdza nierówności w tych językach.

69. A. Wartość %20 służy do kodowania spacji URL przy użyciu schematu kodowania procentowego.

70. C. Wśród innych cech słowo kluczowe rescue do obsługi błędów jest unikalne dla Rubiego.

71. B. Bash i PowerShell umożliwiają bezpośrednie łączenie ciągów i wartości liczbowych. Ruby i Python wymagają jawnej konwersji wartości liczbowych na ciągi przed konkatenacją.

72. D. Nie ma ograniczeń co do liczby klauzul elsif, które mogą być zawarte w skrypcie Rubiego.

73. B. W przypadku wykonywania warunkowego wykonywana jest tylko jedna klauzula. W takim przypadku zostanie wykonany kod następujący po klauzuli if, uniemożliwiając wykonanie klauzuli elif lub else.

74. C. Hasła, pytania zabezpieczające i kody PIN to przykłady uwierzytelniania oparte na wiedzy i nie zapewniałoby wieloczynnikowego uwierzytelniania w połączeniu z hasłem, kolejny czynnik oparty na wiedzy. Aplikacje na smartfony są przykładem „czegoś, co masz” i są akceptowalną alternatywą.

75. D. Streszczenie powinno być napisane w taki sposób, aby było dostępne dla laika. Nie powinien zawierać szczegółów technicznych.

76. A. Naprawa podatności jest działaniem następczym i nie jest przeprowadzana jako część testu. Testerzy powinni jednak usunąć wszelkie powłoki lub inne narzędzia zainstalowane podczas testowania, a także usunąć wszelkie utworzone przez siebie konta lub dane uwierzytelniające.

77. C. Najskuteczniejszym sposobem przeprowadzenia sesji wyciągniętej z lekcji jest poproszenie neutralnej osoby trzeciej, aby służyła jako moderator, umożliwiając każdemu swobodne wyrażanie swoich opinii.

78. D. Zaawansowane trwałe zagrożenie (APT) jest rodzajem aktora zagrożenia, który ma motywację do kradzieży poufnych informacji od głośnych celów przy użyciu zaawansowanych funkcji hakerskich.

79. C. Ryzyko = Prawdopodobieństwo * Potencjalne szkody lub (30 = 6 * 5)

80. B. Biorąc pod uwagę skalę ryzyka od 1 do 100, 30 przypadałoby na skalę o niskim priorytecie.