1. A. Script kiddies to osoba, która przeprowadza atak przy użyciu kodu napisanego przez bardziej zaawansowanych hakerów. Ataki haktywistów są zwykle motywowane politycznie. Aktorzy przestępczości zorganizowanej to zazwyczaj wysoce zorganizowana grupa cyberprzestępców, których głównym celem jest zarobienie dużych pieniędzy. Podmiot zagrażający państwu narodowemu działa w imieniu narodu, aby wyrządzić krzywdę rywalizującemu narodowi.

2. D. Atakujący sponsorowany przez państwo zwykle działa pod kierownictwem agencji rządowej. Ataki są zwykle wymierzone w wykonawców rządowych lub nawet w same systemy rządowe. Skryptowe dziecko to osoba, która przeprowadza atak przy użyciu kodu napisanego przez bardziej zaawansowanych hakerów. Ataki haktywistów są zwykle motywowane politycznie. Aktor grożący przestępczością zorganizowaną to grupa cyberprzestępców, której głównym celem są korzyści finansowe.

3. C. Podmiotem grożącym przestępczością zorganizowaną jest grupa cyberprzestępców, której głównym celem są korzyści finansowe. Ataki przeprowadzane przez zorganizowane grupy przestępcze mogą trwać długo, są bardzo dobrze finansowane i zazwyczaj są dość wyrafinowane. Złośliwy atak z wykorzystaniem informacji poufnych ma miejsce, gdy ktoś w organizacji używa danych uwierzytelniających, które otrzymał w legalny sposób, do przeprowadzenia ataku. Ataki haktywistów są zwykle motywowane politycznie. Podmiot zagrażający państwu narodowemu działa w imieniu narodu, aby wyrządzić krzywdę rywalizującemu narodowi.

4. B. Ataki haktywistów są zwykle motywowane politycznie, a nie finansowo. Zazwyczaj chcą ujawnić postrzeganą korupcję lub zwrócić uwagę na swoją sprawę. Skryptowe dziecko to osoba, która przeprowadza atak przy użyciu kodu napisanego przez bardziej zaawansowanych hakerów. Aktor grożący przestępczością zorganizowaną to grupa cyberprzestępców, której głównym celem są korzyści finansowe. Aktor zagrażający państwu narodowemu działa w imieniu narodu, aby wyrządzić krzywdę rywalizującemu narodowi.

5. D. Złośliwy atak z wykorzystaniem informacji poufnych ma miejsce, gdy ktoś w organizacji wykorzystuje dane uwierzytelniające, które otrzymała zgodnie z prawem, do przeprowadzenia ataku. Skryptowe dziecko to osoba, która przeprowadza atak przy użyciu kodu napisanego przez bardziej zaawansowanych hakerów. Ataki haktywistów są zwykle motywowane politycznie, a nie finansowo. Aktor grożący przestępczością zorganizowaną to grupa cyberprzestępców, której głównym celem są korzyści finansowe.

6. A i B. Nurkowanie w śmietniku to technika wykorzystywana do zbierania informacji o organizacji docelowej poprzez przeglądanie dokumentów znalezionych w jej koszu. Podobnie, theHarvester może być używany do przeszukiwania Internetu w celu znalezienia adresów e-mail i nazwisk pracowników. Informacje te można wykorzystać do stworzenia skutecznej kampanii phishingu włócznią.

7. B i E. Kluczem do udanego wyczynu wielorybniczego jest posiadanie szczegółowych informacji o liderach w organizacji docelowej. Przydatne informacje można często uzyskać ze strony internetowej organizacji w postaci komunikatów prasowych i życiorysów kierownictwa. Te informacje mogą dostarczyć ci nazwiska, stanowiska, a być może nawet dane kontaktowe.

8. A i D. Wywiad o otwartym kodzie źródłowym (OSINT) to wszelkie informacje, które są publicznie dostępne i mogą być gromadzone w sposób pasywny. Ponieważ jest on zbierany pasywnie, nie można używać metod, które aktywnie angażują organizację docelową do gromadzenia OSINT. Na przykład skanowanie podatności jest metodą aktywną, podczas gdy czytanie postów w mediach społecznościowych i przeglądanie zeznań podatkowych od osób prawnych to metody pasywne.

Numery ubezpieczenia społecznego i osobiste zeznania podatkowe są przykładami informacji chronionych, które nie są publicznie dostępne.

9. C i D. Uruchamianie skanowania podatności jest metodą aktywną, podobnie jak penetracja placówki organizacji lub wyłudzanie informacji od niezadowolonego pracownika. Z drugiej strony, zbieranie informacji od rejestratora DNS organizacji lub czytanie ogłoszeń o pracę na stronie internetowej organizacji to przykłady pasywnego gromadzenia informacji publicznych.

10. A i E. Oferty pracy na stronie internetowej organizacji oraz życiorysy obecnych pracowników na LinkedIn są przykładami informacji publicznej. Przeglądając te dwa źródła, możesz określić, jakie typy systemów wdrożyła organizacja.

11. B. W przypadku exploita upuszczania klucza USB, pewien rodzaj złośliwego oprogramowania jest zwykle ładowany na dysk flash. Ten dysk jest następnie celowo pozostawiany w miejscu, w którym prawdopodobnie znajdzie go pracownik docelowej organizacji. Celem jest, aby pracownik podłączył go, aby zobaczyć, co zawiera. Kiedy tak się dzieje, złośliwe oprogramowanie jest automatycznie ładowane na komputer ofiary.

12. A. W przypadku standardowego exploita phishingowego wysyłane są wiadomości e-mail bezkrytycznie do dużej liczby osób, mając nadzieję, że pewien procent z nich kliknie szkodliwy odsyłacz zawarty w wiadomości.

13. C. Atak phishingowy SMS (zwany również atakiem smishing) wykorzystuje wiadomości tekstowe zamiast e-maili do przeprowadzenia exploita phishingowego.

14. A. Głosowy atak phishingowy (zwany również atakiem vishingowym) wykorzystuje połączenie telefoniczne zamiast e-maila do przeprowadzenia exploita phishingowego. Zasadniczo atakujący dzwoni do konkretnego pracownika podszywającego się pod kogoś innego w celu uzyskania informacji.

15. A i D. Zarówno spear phishing, jak i wielorybnictwo wymagają od testera penetracji przeprowadzenia szeroko zakrojonych badań w celu zidentyfikowania osób będących celem ataków o wysokiej wartości w organizacji.

16. A. Polecenie nmap 192.168.1.10-13 -sA powoduje, że narzędzie nmap przeprowadza skanowanie TCP ACK systemów docelowych z adresami IP 192.168.1.10, 192.168.1.11 i 192.168.1.13.

17. C. Ponieważ skanowane hosty nie mają ciągłych adresów IP, należy określić każdego hosta indywidualnie. W tym przypadku polecenie nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 -sU powoduje, że narzędzie nmap przeprowadza skanowanie portów UDP każdego określonego systemu.

18. B. Polecenie nmap 192.168.1.1-254 -sn powoduje, że narzędzie nmap skanuje określony zakres adresów IP w poszukiwaniu hostów. Zawiera listę wszystkich znalezionych hostów bez faktycznego skanowania ich portów.

19. D. Polecenie nmap 192.168.1.1-254 –p 23 powoduje, że narzędzie nmap skanuje określony zakres adresów IP w poszukiwaniu hostów z otwartym portem Telnet 23.

20. A. Polecenie nmap 192.168.1.2 -p- powoduje, że narzędzie nmap skanuje wszystkie porty na określonym hoście. Należy pamiętać, że skanowanie zajmie trochę czasu ze względu na liczbę zaangażowanych portów.

21. B. Termin usuwanie konfliktów odnosi się do procesu komunikacji między klientem a testerem w celu ustalenia, czy atak wykryty podczas testu penetracyjnego jest w rzeczywistości częścią autoryzowanego testu penetracyjnego, czy też został zainicjowany przez stronę trzecią haker.

22. D. Termin deeskalacja odnosi się do procesu komunikacji między klientem a testerem w celu zmniejszenia intensywności exploitów lub nawet powstrzymania ich wszystkich razem z powodu niebezpiecznych sytuacji, które mogą powodować.

23. B. Termin zaufany agent odnosi się do osoby w celu organizacji, zazwyczaj administrator IT lub menedżer, który ma bezpośrednią linię komunikacji z testerem penetracyjnym. Osoba ta jest zwykle odpowiedzialna za komunikację między klientem a testerem w celu usunięcia konfliktu i eskalacji.

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

25. 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.

26. C. Język Web Application Description Language (WADL) jest opartym na XML-u, czytelnym maszynowo opisem usług internetowych opartych na HTTP. W związku z tym jest zwykle używany z usługami REST zamiast SOAP.

27. B i D. Dokumentacja interfejsu programowania aplikacji (API) opisuje sposób komunikowania się komponentów oprogramowania. Zestawy programistyczne (SDK) są również dostarczane z dokumentacją. Organizacje mogą tworzyć własne pakiety SDK, korzystać z komercyjnych pakietów SDK lub korzystać z pakietów SDK typu open source. Zrozumienie, które pakiety SDK są w użyciu i gdzie się znajdują, może pomóc testerowi penetracji testować aplikacje, zwłaszcza te napisane we własnym zakresie.

28. D. Test penetracji czarnej skrzynki powinien symulować widok sieci, jaki miałby atakujący z zewnątrz. Dlatego tester powinien mieć niewielką lub żadną wiedzę o sieci wewnętrznej.

29. D. W teście białej skrzynki powinieneś mieć dostęp do obszernej dokumentacji wewnętrznej. Ponieważ jako wektor ataku zostanie użyta aplikacja opracowana wewnętrznie, należy wymagać od klienta dostarczenia jak największej ilości dokumentacji na temat tej aplikacji. Na przykład należy poprosić o diagramy architektoniczne, przykładowe żądania aplikacji i dokument swagger, jeśli ma to zastosowanie.

30. C i E. Gdy zamawiasz wewnętrzne diagramy architektoniczne w ramach testu białej skrzynki, zazwyczaj powinieneś otrzymać dokumentację, taką jak diagramy sieciowe i mapy obiektów. Informacje te można wykorzystać do mapowania topologii sieci i lokalizacji kluczowych urządzeń infrastruktury, takich jak przełączniki, routery i serwery

31. A. Jedną z opcji, którą możesz wypróbować w tym scenariuszu, jest dekompilacja plik wykonywalny aplikacji. Ten proces ujawni kod poziomu montażu aplikacji, który możesz przeanalizować pod kątem słabości.

32. B. Większość dekompilatorów tworzy kod źródłowy na poziomie asemblera, a nie kod C++. Aby ta informacja była użyteczna, potrzebujesz dużego doświadczenia w pracy z kodem języka asemblerowego. Zazwyczaj będzie to wymagało zatrudnienia konsultanta z rozległą wiedzą na temat programowania w asemblerze.

33. B. Debugery umożliwiają analizowanie aplikacji podczas jej wykonywania. Zazwyczaj można wstrzymać wykonywanie aplikacji krok po kroku lub zezwolić na jej działanie, dopóki nie osiągnie określonego punktu w kodzie. W ten sposób możesz zidentyfikować lukę, którą można wykorzystać w ramach testu penetracyjnego. Jednak, aby robić to skutecznie, musisz mieć duże doświadczenie w programowaniu lub testowaniu aplikacji.

34. A. Zespół reagowania na incydenty komputerowe (CERT) rządu Stanów Zjednoczonych prowadzi stronę internetową pod adresem http://www.us-cert.gov, która zawiera regularnie aktualizowane podsumowanie najczęściej zgłaszanych obecnie rodzajów incydentów związanych z bezpieczeństwem. do CERT.

35. B. JPCERT to rządowa wersja USA Rządowego Zespół Reagowania na Awarie Komputerowe (CERT). JPCERT prowadzi stronę internetową pod adresem https://www .jpcert.or.jp/english/, która zapewnia dynamiczne podsumowanie bieżących alertów i porad dotyczących bezpieczeństwa.

36. D i E. Exploity EternalBlue i WannaCry są ułatwione przez słabości protokołu SMB. Exploit EternalBlue wykorzystuje fakt, że SMBv1 niewłaściwie obsługuje pakiety exploitów, umożliwiając atakującym zdalne wykonanie złośliwego kodu w systemie z uruchomionym protokołem SMB. WannaCry to forma oprogramowania ransomware, które wykorzystuje EternalBlue, aby uzyskać dostęp do podatnych systemów i zainstalować się.

37. C i E. Protokół SMB używa portów TCP 139 i 445. System z tymi dwoma portami jest najprawdopodobniej hostem Windows z SMB lub hostem Linux z Sambą (która jest implementacją usługi SMB typu open source).

38. A i B. Protokół SNMPv1 jest starszym protokołem, który wykorzystuje koncepcję ciągu społeczności zamiast hasła. Ten sam ciąg wspólnoty jest używany do uwierzytelniania na każdym hoście SNMPv1 w sieci. Zgodnie z konwencją większość administratorów SNMPv1 ustawia ciąg wspólnoty na wartość public. Nawet jeśli użyto unikalnego ciągu społeczności, łatwo było go wykryć, ponieważ był przesyłany w sieci jako czysty tekst.

39. A. Protokół SNMP działa na porcie UDP 161.

40. B. Protokół SMTP służy do przesyłania wiadomości e-mail między agentami przesyłania poczty (MTA).

41. B. Social Engineer Toolkit (SET) to narzędzie do testowania penetracji o otwartym kodzie źródłowym przeznaczone do przeprowadzania exploitów socjotechnicznych.

42. A. Browser Exploitation Framework (BeEF) to narzędzie do testowania penetracji zaprojektowane w celu wykorzystania słabości przeglądarek internetowych za pomocą ataków po stronie klienta.

43. D. Narzędzie ncat może być używane do odczytu, zapisu, przekierowywania i szyfrowania danych sieciowych. Na przykład może służyć do ustanawiania sesji powłoki z różnymi serwerami, w tym z systemami Windows, Linux i UNIX.

44. A i B. Do dekompilacji można użyć zarówno IDA, jak i Hoppera. Podczas tego procesu plik wykonywalny jest wstecznie kompilowany do kodu źródłowego, co pozwala na zbadanie go pod kątem luk.

45. C i E. Zarówno pierwszy, jak i FTK są narzędziami kryminalistyki. Służą do zbierania i analizowania dowodów cyfrowych z miejsca cyberprzestępczości.

46. D. Ustawienie zasad grupy „Maksymalny wiek hasła” określa, jak długo użytkownik może przechowywać to samo hasło, zanim będzie musiał zmienić je na nowe. Po upływie tego czasu użytkownik jest zmuszony do utworzenia nowego hasła.

47. C. Ustawienie zasad grupy „Minimalny wiek hasła” określa, jak długo użytkownik musi przechowywać to samo hasło, zanim będzie mógł je zmienić na nowe. Do tego czasu użytkownik jest zmuszony do zachowania tego samego hasła. Uniemożliwia to użytkownikom dokonywanie ciągłych zmian hasła w celu obejścia ustawienia „Egzekwuj zasady historii haseł”.

48. A. Polecenia chage można użyć w systemach Linux do skonfigurowania przedawniania haseł dla kont użytkowników.

49. D. Ustawienie zasad grupy „Próg blokady konta” określa liczbę nieudanych prób logowania, które użytkownik może wykonać przed zablokowaniem konta. Zablokowanego konta nie można użyć ponownie, dopóki nie zostanie odblokowane przez administratora lub nie upłynie okres blokady konta. To ustawienie zasad może pomóc w zapobieganiu atakom siłowym, blokując konto po zaledwie kilku próbach zgadywania.

50. B. Ustawienie zasad grupy „Czas blokady konta” określa, jak długo zablokowane konto pozostaje zablokowane przed automatycznym odblokowaniem. To ustawienie zasad pomaga zapobiegać atakom siłowym, znacznie zwiększając ilość czasu wymaganego do przeprowadzenia ataku.

51. C. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiednich celów triady DAD. Drugie D w DAD oznacza odmowę, która odnosi się do zapobiegania legalnemu wykorzystaniu informacji lub systemów.

52. A. Testerzy penetracji starają się podważyć cele modelu triady CIA przy użyciu odpowiadających im celów triady DAD. Pierwsze D w DAD oznacza ujawnienie, które odnosi się do uzyskania nieuprawnionego dostępu do informacji lub systemów. W tym scenariuszu Robert uzyskał dostęp do informacji w wewnętrznej bazie danych, do których nie powinien mieć dostępu.

53. C. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiednich celów triady DAD. Litera A w DAD oznacza zmianę, która odnosi się do dokonywania nieautoryzowanych zmian w informacjach lub systemach. W tym scenariuszu Robert zmienił system uwierzytelniania, dodając konto nieautoryzowanego użytkownika.

54. D. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiednich celów triady DAD. Drugie D w DAD oznacza odmowę, która odnosi się do zapobiegania legalnemu wykorzystaniu informacji lub systemów. W tym scenariuszu Robert przeprowadził atak odmowy usługi (DoS) na serwer plików, odmawiając legalnego dostępu do niego.

55. C. Atakujący (i testerzy penetracji) dążą do podważenia celów modelu triady CIA przy użyciu odpowiednich celów triady DAD. Litera A w DAD oznacza zmianę, która odnosi się do dokonywania nieautoryzowanych zmian w informacjach lub systemach. W tym scenariuszu Robert zmienił system rozliczania wynagrodzeń pracowników.

56. B. Host najprawdopodobniej działa w systemie Windows. Porty TCP 139, 445 i 3389 są powszechnie używane w usługach udostępniania plików systemu Windows. Chociaż te porty mogą być również używane w innych systemach operacyjnych (takich jak system Linux z uruchomionym demonem SMB), bardziej prawdopodobne jest, że będzie to host systemu Windows.

57. D. Host jest prawdopodobnie serwerem WWW. Administrator systemu prawdopodobnie zmienił domyślne porty serwera WWW na porty niestandardowe, próbując ukryć jego funkcję. Jest to przykład „bezpieczeństwa przez ukrywanie”.

58. C. Opcja -T konfiguruje szybkość, z jaką nmap uruchamia skanowanie podatności. W tym scenariuszu podsieć jest potencjalnie ogromna, z ponad 16 milionami możliwych adresów IP. Uruchomienie nmapa z opcją –T0 w tak dużej podsieci zajmie dużo czasu.

59. A. Whois może potencjalnie ujawnić wiele informacji o organizacji docelowej, w tym:

Rejestrator domen

Nazwa prawna rejestrującego

Adres rejestrującego

Numer telefonu abonenta

Kontaktowy adres e-mail

Imię i nazwisko administratora domeny

Niektóre organizacje proszą swojego rejestratora o ukrycie tych informacji przed opinią publiczną.

60. C. W tym scenariuszu przeprowadzany jest test penetracji czarnej skrzynki. Z definicji tester znajduje się gdzieś poza siecią celu. W związku z tym musi najpierw skompromitować hosta wewnętrznego. Po zakończeniu może się obracać i używać go do skanowania innych hostów wewnętrznych.

61. A i B. Zarówno przechowywane/trwałe, jak i odzwierciedlane exploity XSS są uważane za exploity po stronie serwera, ponieważ złośliwe skrypty są osadzone na serwerze. Gdy użytkownik przegląda stronę internetową, złośliwe skrypty są uruchamiane, umożliwiając atakującemu przechwycenie informacji lub wykonanie innych działań.

62. B. Jest to przykład fałszerstwa żądań między witrynami (CSRF). Ponieważ sesyjny plik cookie ze strony internetowej został zapisany lokalnie, użytkownik jest na stałe zalogowany w witrynie. W związku z tym żądanie HTTP zmiany hasła użytkownika zawarte w wiadomości e-mail nie wymagało uwierzytelnienia do wykonania. Tester penetracyjny może teraz zalogować się do Active Directory jako pracownik wysokiego szczebla.

63. C. W przypadku exploita typu clickjacking tester dodaje przezroczyste warstwy do strony internetowej, próbując nakłonić użytkownika do kliknięcia ukrytego przycisku lub łącza na przezroczystej warstwie. Dzięki temu tester może przejąć kliknięcia użytkownika i wysłać je do innej witryny (np. witryny do zbierania danych uwierzytelniających).

64. A. Jeśli przechodzenie katalogów zostało dozwolone w konfiguracji serwera WWW, może potencjalnie ujawnić system plików serwera WWW użytkownikom uzyskującym dostęp do witryny w przeglądarce internetowej, w tym katalogów poza katalogiem głównym serwera WWW. Na przykład serwer WWW Apache można uruchomić w więzieniu chroot, aby uniemożliwić użytkownikom dostęp do katalogów poza katalogami serwera WWW.

65. B. Manipulacja plikami cookie to błędna konfiguracja zabezpieczeń po stronie klienta, która umożliwia skryptowi działającemu w przeglądarce zapisywanie danych w pliku cookie po stronie klienta.

66. C. Operatora relacyjnego -ge można użyć zarówno w Bash, jak i PowerShell, aby sprawdzić, czy jedna wartość jest liczbowo większa lub równa drugiej.

67. B. Operatora relacyjnego -gt można użyć zarówno w Bash, jak i PowerShell, aby sprawdzić, czy jedna wartość jest liczbowo większa od drugiej.

68. A. Operator relacyjny >= może być użyty zarówno w Pythonie, jak iw Ruby do sprawdzenia, czy jedna wartość jest liczbowo większa lub równa drugiej.

69. B. Operatora relacyjnego -lt można użyć zarówno w Bash, jak i PowerShell, aby sprawdzić, czy jedna wartość jest liczbowo mniejsza od drugiej.

70. D. Operator relacyjny < może być użyty zarówno w Pythonie, jak iw Ruby do sprawdzenia, czy jedna wartość jest numerycznie mniejsza od drugiej.

71. A. Po teście penetracyjnym bardzo ważne jest, aby poinformować klienta o tym, co się wydarzyło i co zostało odkryte. Podczas procesu atestacji ustaleń przekazujesz klientowi szczegółowe dowody tego, co odkryłeś. Klient może następnie wykorzystać te informacje do naprawienia znalezionych problemów.

72. C. Po zakończeniu testu penetracyjnego, tester często prosi klienta o wyrażenie zgody (zazwyczaj na piśmie), że tester wypełnił umowę, która została pierwotnie podpisana z klientem. Proces ten nazywa się akceptacją klienta.

73. C. Po zakończeniu testu penetracyjnego często zdarza się, że klient prosi testera, aby wrócił i ponownie przetestował wszystko, aby upewnić się, że problemy wykryte podczas testu zostały naprawione. Ten proces jest czasami nazywany działaniami następczymi.

74. A i C. Po zakończeniu testu penetracyjnego powinieneś spotkać się ze swoimi zespołami i omówić wyciągnięte wnioski. Powinieneś określić, co poszło dobrze i jakie ulepszenia należy wprowadzić. Na przykład powinieneś omówić, które exploity działały, a które nie. Powinieneś udokumentować najlepsze praktyki korzystania z tych exploitów, aby nie trzeba było ich ponownie uczyć się przy następnym przeprowadzaniu testu penetracyjnego.

75. C. Common Vulnerability Scoring System (CVSS) to branżowy standard oceny powagi luk w zabezpieczeniach. Zapewnia technikę oceniania każdej luki w różnych miarach. Analitycy bezpieczeństwa często używają ocen CVSS do ustalania priorytetów działań związanych z odpowiedzią. Każdy środek otrzymuje ocenę opisową i punktację liczbową.

76. A. Do generowania kluczy służy polecenie ssh-keygen. Aby porównać wartości klucza prywatnego i publicznego, należy wygenerować klucz publiczny z klucza prywatnego przy użyciu następującej składni: ssh-keygen -y -f <klucz prywatny>. Następnie możesz odczytać zawartość pliku Author_keys i porównać/skontrastować ewentualne różnice. Odpowiedź B wygeneruje parę kluczy prywatnych i publicznych RSA o długości 2048 bitów. Odpowiedź C odczyta i rozróżni zawartość klucza publicznego i prywatnego; jednak nie są to te same kluczowe wartości, więc to nie zadziała. Odpowiedź D jest nieprawidłowa, ponieważ openssl zweryfikuje zawartość klucza RSA i prześlij dane wyjściowe polecenia wraz z danymi wyjściowymi polecenia cat id_rsa.pub na ekran, co nie pomoże w znalezieniu wartości klucza publicznego z zaatakowanego klucza prywatnego RSA.

77. C. Ciągnięcie wytrycha symuluje technikę jigglingu. Gdy spust jest pociągnięty, głowica pick-pistoleta uderza o bolce klucza, zmuszając je do podniesienia. Następnie, po zwolnieniu spustu, głowica opada, umożliwiając grawitacji i sprężynom w komorze kręgli wepchnięcie kręgli z powrotem na miejsce i niemal natychmiast głowica pistoletu uderza w kręgle, a wszystko to przy odpowiednim

nacisku na kręgle. klucz napinający. Grabienie (lub szorowanie) to ruch do przodu i do tyłu w rowku, a SPP to technika testowania pinów, która wymaga wielu umiejętności i cierpliwości.

78. C. Styropian jest dobrym izolatorem i może być używany podczas fizycznego testu penetracyjnego, aby chronić temperaturę ciała przed wystawieniem na działanie pasywnego czujnika ciepła na podczerwień.

79. A. Niektóre rodzaje zamków szyfrowych można pokonać za pomocą magnesu o dużej mocy. Ta metoda jest mniej destrukcyjna, wymaga niewielkiego wysiłku i jest rozsądna z punktu widzenia medycyny sądowej. Młotek jest dobrą opcją; wymaga jednak silnego wejścia i może zrobić prawdziwy bałagan na drzwiach. W tym scenariuszu śrubokręt może zdziałać bardzo niewiele, a brutalna siła może być rozsądną metodą kryminalistyczną, ale pomyślne wykonanie może zająć dużo czasu.

80. B. Moduły Metasploit stosują dość stałą praktykę usuwania wszystkiego, co zostało dodane do dysku, czego jeszcze tam nie było. Ułatwia to sprawę i zapewnia pewien poziom pewności podczas wykonywania sesji — K, aby zabić wszystkie sesje za pośrednictwem konsoli Metasploit.