1. Którzy z poniższych napastników z największym prawdopodobieństwem będą w stanie przeprowadzić zaawansowane trwałe zagrożenie (APT)? (Wybierz dwa.)

A. Złośliwy insider

B. Script kiddie

C. Haktywista

D. Przestępczość zorganizowana

E. Państwo narodowe

2. Które z poniższych podmiotów z największym prawdopodobieństwem staną się celem zaawansowanego trwałego zagrożenia (APT)? (Wybierz dwa.)

A. Wykonawca rządowy

B. Witryna oferująca lekcje na temat optymalizacji pod kątem wyszukiwarek (SEO)

C. Bank wielonarodowy

D. Gabinet stomatologiczny

E. Kolegium społeczne

3. Który podmiot zagrażający najprawdopodobniej kieruje się sprawą polityczną?

A. Złośliwy insider

B. Haktywista

C. Przestępczość zorganizowana

D. Script kiddie

4. Który aktor zagrażający najprawdopodobniej kieruje się chęcią zwrócenia na siebie uwagi?

A. Złośliwy insider

B. Script kiddie

C. Przestępczość zorganizowana

D. Państwo narodowe

5. Jaki rodzaj testu penetracyjnego zazwyczaj zapewnia najdokładniejszą ocenę w najkrótszym czasie?

A. Ocena szarej skrzynki

B. Ocena czarnej skrzynki

C. Ocena oparta na celach

D. Ocena białej skrzynki

6. Znajdujesz się na etapie zbierania informacji w ramach testu penetracyjnego czarnej skrzynki. Jakich narzędzi możesz użyć, aby wyznaczyć organizację docelową za pomocą OSINT? (Wybierz dwa.)

A. aircrack-ng

B. whois

C. rozpoznanie

D. Kismet

E. Wi-Fiight

7. Rozważ dane wyjściowe z polecenia pokazanego tutaj:

Które narzędzie OSINT zostało użyte do zebrania tych informacji?

A. whois

B. nslookup

C. nmap

D. ifconfig

E. host

8. Rozważ dane wyjściowe z polecenia pokazanego tutaj:

Które narzędzie OSINT zostało użyte do zebrania tych informacji?

A. whois

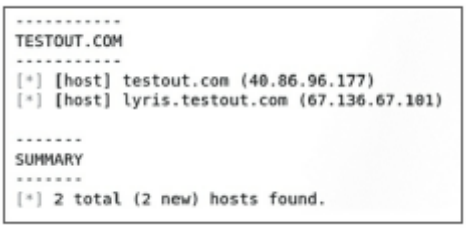
B. nslookup

C. Nessusa

D. recon-ng

E. host

9. Rozważ wynik polecenia pokazanego tutaj:



Które narzędzie OSINT zostało użyte do zebrania tych informacji?

A. whois

B. nslookup

C. nmap

D. recon-ng

E. host

10. Przeprowadzasz rekonesans w ramach testu penetracji czarnej skrzynki. Uruchamiasz skanowanie luk w zabezpieczeniach na jednym z publicznych serwerów docelowej organizacji i odkrywasz, że port 25 jest otwarty. Na co to wskazuje?

A. Jest to serwer DNS.

B. Jest to serwer SMTP.

C. Jest to serwer FTP.

D. Jest to serwer plików SMB.

11. Która technika socjotechniki jest najrzadziej stosowana podczas testu penetracyjnego?

A. Przesłuchanie

B. Podszywanie się

C. Surfowanie na ramieniu

D. Upuszczenie klucza USB

12. Zostałeś zatrudniony do przeprowadzenia dla klienta testu penetracyjnego z wykorzystaniem czarnej skrzynki. Kupujesz mały dysk flash i ładujesz go złośliwym oprogramowaniem, które wysyła do Ciebie informacje. Korzystając z technik rozpoznawczych, zidentyfikowałeś dostawcę, który obsługuje ogrzewanie i klimatyzację w centrali organizacji. Ubierasz się w podobny strój jak pracownicy tego sprzedawcy i kupujesz narzędzia, których zwykle używają. Recepcjonistka organizacji docelowej umożliwia wejście i kieruje do pomieszczenia technicznego. Celowo zostawiasz pamięć flash na krześle

użytkownika, przechodząc obok otwartej kabiny. Jakie exploity zostały wykorzystane w tym scenariuszu?

(Wybierz dwa.)

A. Pozyskiwanie

B. Podszywanie się

C. Surfowanie na ramieniu

D. Upuszczenie klucza USB

E. Kompromis biznesowej poczty e-mail

13. Zostałeś wynajęty do przeprowadzenia testu penetracyjnego czarnej skrzynki dla klienta. Wchodzisz do głównego wejścia organizacji i pytasz recepcjonistkę o informacje o aktualnych ofertach pracy. Oglądasz naciśnięcia klawiszy, które wpisuje na swoim komputerze, w nadziei na przechwycenie poufnych informacji, których możesz użyć, aby uzyskać dostęp do sieci wewnętrznej. Jaki rodzaj exploita wykorzystano w tym scenariuszu?

A. Spear phishing

B. Podszywanie się

C. Surfowanie na ramieniu

D. Upuszczenie klucza USB

E. Kompromis biznesowej poczty e-mail

14. Zostałeś zatrudniony do przeprowadzenia testu penetracyjnego szarej skrzynki dla klienta. Udało ci się przejść, gdy logowała się na swoje konto e-mail i obserwowała naciśnięcia klawiszy, które wpisywała na swoim komputerze. Później tego samego wieczoru, gdy pracownik wyszedł na cały dzień do domu, logujesz się na jej konto e-mail i wysyłasz prośby o informacje do innych pracowników. Jakie exploity zostały wykorzystane w tym scenariuszu? (Wybierz dwa.)

A. Spear phishing

B. Wielorybnictwo

C. Upuszczenie klucza USB

D. Surfowanie po ramieniu

E. Kompromis biznesowej poczty e-mail

15. Przeprowadzasz rekonesans w ramach testu penetracji czarnej skrzynki. Zauważasz, że pracownicy organizacji docelowej często gromadzą się w określonej restauracji na świeżym powietrzu na lunch. Zaczynasz odwiedzać tę samą restaurację na lunch i zaprzyjaźnić się z kilkoma pracownikami docelowej organizacji. Po zdobyciu ich zaufania zaczynają udostępniać informacje o swojej pracy, komputerach, szefach, klientach, projektach i tak dalej. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. Whaling

B. Elicitation

C. Interrogation

D. Phishing

16. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Użyj narzędzia nmap, aby sprawdzić, czy usługa Telnet działa na wykrytym serwerze Linux. Dane wyjściowe polecenia wskazują, że stan portu Telnet jest filtrowany. Co to prawdopodobnie oznacza?

A. Usługa Telnet jest zainstalowana, ale nie działa.

B. Usługa Telnet nie jest zainstalowana.

C. Usługa Telnet nie jest zainstalowana, a inna usługa używa swojego portu domyślnego.

D. Usługa Telnet jest zainstalowana i działa, ale blokuje ją zapora hosta.

17. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Użyj narzędzia nmap, aby sprawdzić, czy usługa Telnet działa na wykrytym serwerze Linux. Dane wyjściowe polecenia wskazują, że stan portu Telnet to Otwarty. Co to znaczy?

A. Usługa Telnet jest zainstalowana, ale nie działa.

B. Usługa Telnet jest zainstalowana, uruchomiona i dostępna.

C. Usługa Telnet nie jest zainstalowana, a inna usługa używa swojego portu domyślnego.

D. Usługa Telnet nie jest zainstalowana.

18. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Użyj narzędzia nmap, aby sprawdzić, czy usługa Telnet działa na wykrytym serwerze Linux. Dane wyjściowe polecenia wskazują, że stan portu Telnet jest zamknięty. Co to może oznaczać? (Wybierz dwa.)

A. Usługa Telnet jest zainstalowana, ale nie działa.

B. Usługa Telnet jest zainstalowana, uruchomiona i dostępna.

C. Usługa Telnet nie jest zainstalowana, a inna usługa używa swojego portu domyślnego.

D. Usługa Telnet nie jest zainstalowana.

E. Usługa Telnet jest zainstalowana i działa, ale blokuje ją zapora hosta.

19. Tester penetracyjny używa narzędzia nmap do wysłania pakietu TCP SYN do hosta docelowego. Host docelowy odpowiada pakietem SYN ACK, ale zamiast zakończyć połączenie, nmap wysyła pakiet resetujący do hosta docelowego. Której opcji tester użył z poleceniem nmap?

A. -sS

B. -sT

C. -sU

D. -sL

20. Która opcja polecenia powoduje, że nmap wykrywa usługi działające na hoście docelowym i zgłasza numer wersji znalezionych usług?

A. -sS

B. -sT

C. -sU

D. -sV

21. Przeprowadzasz test penetracyjny białej skrzynki dla klienta. Podczas testu odkryjesz ukryte konto administratora backdoora na jednym z kontrolerów domeny Active Directory klienta. Sprawdzasz dzienniki kontrolera domeny i stwierdzasz, że konto backdoora jest codziennie aktywnie używane. Zamiast czekać do końca testu, natychmiast komunikujesz się z klientem, aby ostrzec go, że jego serwer został naruszony. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Etapy

B. Krytyczne ustalenia

C. Ścieżka komunikacyjna

D. Wskaźniki wcześniejszego kompromisu

22. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta. Faza wyliczania testu została zakończona i możesz rozpocząć wykorzystywanie podatnych systemów. Zanim to zrobisz, komunikujesz się z klientem i informujesz go, że test przechodzi. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Ocena ryzyka

B. Krytyczne ustalenia

C. Ustalenia i środki zaradcze

D. Etapy

23. Przeprowadzasz test penetracyjny białej skrzynki dla klienta. Podczas testu zauważysz wychodzący ruch sieciowy zgodny z atakiem rozproszonej odmowy usługi (DDoS). Podejrzewasz, że wewnętrzne systemy zostały zainfekowane złośliwym oprogramowaniem, tworząc sieć wzmacniaczy do ataku. Zamiast czekać do końca testu, natychmiast komunikujesz się z klientem, aby go ostrzec. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Etapy

B. Wskaźniki wcześniejszego kompromisu

C. Ustalenia i środki zaradcze

D. Krytyczne ustalenia

24. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Podczas testu okazuje się, że technicy pomocy technicznej używają uwierzytelnionych, ale nieszyfrowanych połączeń FTP przez Internet do przesyłania plików na komputery znajdujące się w zdalnych oddziałach firmy. W związku z tym ich poświadczenia są potencjalnie ujawniane w sieci publicznej. Mimo że stanowi to kuszący cel, który możesz wykorzystać, zdajesz sobie sprawę z bezpośredniego ryzyka związanego z tą praktyką. Zamiast czekać do końca testu, natychmiast komunikować się z klientem, aby ostrzec go, że poświadczenia uprzywilejowane mogą zostać ujawnione w Internecie. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Etapy

B. Krytyczne ustalenia

C. Ścieżka komunikacyjna

D. Wskaźniki wcześniejszego kompromisu

25. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta. Test jest teraz zakończony i możesz rozpocząć sprzątanie po sobie. Zanim to zrobisz, komunikujesz się z klientem i informujesz go, że test został ukończony i masz świadomość, że nastąpi aktywacja czyszczenia. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Ocena ryzyka

B. Krytyczne ustalenia

C. Etapy

D. Wskaźniki wcześniejszego kompromisu

26. Sprawdzasz dla klienta test penetracyjny białej skrzynki. Celem jest sprawdzenie, czy możesz uzyskać dostęp do poufnych danych badawczych przechowywanych na wewnętrznym serwerze bazy danych. Aby to ułatwić, zażądałeś, aby klient zapewnił Ci dostęp do aplikacji, których użytkownicy końcowi używają do generowania przykładowych żądań aplikacji. Które konkretnie aplikacje powinny być uwzględnione w żądaniu? (Wybierz dwa.)

A. Opracowana wewnętrznie aplikacja komputerowa służąca do uzyskiwania dostępu do informacji przechowywanych w bazie danych

B. Microsoft Word, którego użytkownicy końcowi używają na co dzień do komponowania dokumentów przechowywanych w bazie danych

C. Microsoft Excel, którego użytkownicy końcowi używają na co dzień do tworzenia arkuszy kalkulacyjnych przechowywanych w bazie danych

D. Własna aplikacja internetowa służąca do generowania raportów z wykorzystaniem informacji przechowywanych w bazie danych

E. Adobe Photoshop, którego użytkownicy końcowi używają na co dzień do edycji plików graficznych zapisanych w bazie danych

27. Chcesz wygenerować przykładowe żądania aplikacji dla własnej aplikacji internetowej, z której użytkownicy klienta korzystają na co dzień do wykonywania swoich codziennych zadań. Jak należy to zrobić?

A. Wprowadź dokładnie te same dane do aplikacji internetowej, które wprowadzają użytkownicy końcowi.

B. Wprowadź dane, które są podobne do danych, które użytkownicy końcowi wprowadzają do aplikacji.

C. Wprowadź do aplikacji zupełnie nieoczekiwane dane.

D. Poproś administratora systemu o wygenerowanie próbek dla Ciebie.

28. Która z poniższych specyfikacji jest specyfikacją protokołu przesyłania wiadomości, która określa, w jaki sposób ustrukturyzowane informacje mogą być wymieniane między aplikacjami internetowymi i są tworzone na podstawie plików WSDL?

A. SOAP

B. XSD

C. WADL

D. Swagger

29. Która z poniższych jest platformą open source, która ma pomóc programistom w projektowaniu, budowaniu, dokumentowaniu i testowaniu usług internetowych Representational State Transfer (REST)?

A. SOAP

B. XSD

C. WSDL

D. Swagger

30. Na którym z poniższych protokołów jest oparta architektura aplikacji internetowej Representational State Transfer (REST)?

A. FTP

B. HTTP

C. MSP

D. LDAP

31. Które źródło badań o otwartym kodzie źródłowym jest utrzymywane przez Narodowy Instytut Nauki i Technologii rządu USA i zawiera podsumowanie aktualnych zabezpieczeń?

A. CERT

B. Pełne ujawnienie

C. CVE

D. NVD

32. Które źródło badań typu open source jest wspólną bazą danych opracowaną przez społeczność, używaną przez dostawców branżowych na całym świecie do zgłaszania luk w zabezpieczeniach i ekspozycji związanych z ich produktami?

A. CERT

B. JPCERT

C. CVE

D. CAPEC

33. Które źródło badań typu open source jest wspólną bazą danych opracowaną przez społeczność, która zawiera luki w zabezpieczeniach i zagrożenia związane ogólnie z oprogramowaniem, a nie z produktem konkretnego dostawcy?

A. CERT

B. Pełne ujawnienie

C. CWE

D. CAPEC

34. Które źródło badań typu open source to stworzona przez społeczność wspólna baza danych zawierająca opisy powszechnie stosowanych wzorców cyberataków?

A. CERT

B. CWE

C. CVE

D. CAPEC

35. Które źródło badań typu open source jest publikowane przez organizację, która produkuje narzędzie nmap?

A. CERT

B. Pełne ujawnienie

C. CVE

D. NVD

36. Podczas testu penetracyjnego szarej skrzynki odkrywasz otwartą usługę SMTP działającą na starszym serwerze bazy danych. Chcesz używać tej usługi SMTP do wysyłania e-maili phishingowych do użytkowników w organizacji. Jak nazywa się ten exploit?

A. Distributed denial of service

B. SMTP relay

C. Fraggle

D. Teardrop

37. Podczas testu penetracyjnego szarej skrzynki odkrywasz otwartą usługę SMTP działającą na starszym serwerze bazy danych. Chcesz korzystać z tej usługi SMTP, aby wysyłać e-maile dotyczące wielorybów do dyrektora generalnego i dyrektora finansowego organizacji. Jak możesz to zrobić zdalnie z laptopa?

A. Telnet z adresem IP serwera SMTP na porcie 25 i utwórz wiadomości.

B. Użyj fizycznych luk bezpieczeństwa, aby uzyskać dostęp do konsoli serwera, gdzie możesz tworzyć wiadomości.

C. Użyj personifikacji, aby nakłonić administratora serwera do ujawnienia hasła do pulpitu zdalnego.

D. Żadne z powyższych.

38. Jakich portów używa serwer FTP? (Wybierz dwa.)

A. 20

B. 21

C. 22

D. 23

E. 25

39. Podczas wykonywania testu penetracji czarnej skrzynki identyfikujesz znaczną ilość danych FTP przesyłanych między nieznanym hostem wewnętrznym w sieci docelowej a hostami w Internecie na portach 20 i 21. Jak wykorzystać ten ruch, aby uzyskać dostęp do systemy w sieci docelowej?

A. Przeprowadź rozproszony atak typu „odmowa usługi" (DDoS).

B. Przeprowadź atak lądowy.

C. Przechwytuj ruch FTP za pomocą sniffera.

D. Użyj anonimowego dostępu do FTP, aby przesłać keylogger na serwer FTP.

40. Przeprowadzasz test penetracyjny szarej skrzynki. Chcesz przechwycić dane uwierzytelniające kierowników Clevel. Aby to osiągnąć, konfigurujesz fałszywy wewnętrzny serwer sieciowy, który wygląda dokładnie tak, jak serwer sieciowy używany do zarządzania wnioskami o zwolnienie pracowników i zwrot kosztów. Wstrzykujesz fałszywy rekord DNS na serwer DNS organizacji, który przekierowuje ruch z prawdziwego serwera na Twój fałszywy serwer. Jak nazywa się ten exploit?

A. Zatrucie DNS

B. Zatrucie ARP

C. Phishing

D. Whaling

41. Którego z poniższych narzędzi może użyć administrator systemu, aby zapewnić zgodność sieci z konfiguracją?

A. Nikto

B. Tableau

C. AFL

D. IDA Pro

42. Podczas testu penetracyjnego czarnej skrzynki musisz użyć uchylania się, aby ukryć swoją obecność przed administratorami systemu w organizacji docelowej. Jakiego narzędzia możesz użyć, aby to zrobić?

A. YASCA

B. SonarQube

C. SAST

D. proxychains

43. Które z poniższych narzędzi można wykorzystać do debugowania lub dekompilacji pliku wykonywalnego systemu Android? (Wybierz dwa.)

A. Studio APK

B. Olydbg

C. Debuger odporności

D. APKX

E. GDB

44. Które z poniższych narzędzi można wykorzystać w ramach procesów zapewniania oprogramowania do przeprowadzania testów rozmytych aplikacji? (Wybierz dwa.)

A. AFL

B. Olydbg

C. Debuger odporności

D. Brzoskwinia

E. GDB

45. Które z poniższych narzędzi można wykorzystać w ramach procesów zapewniania oprogramowania do wykonywania testów SAST i DAST? (Wybierz dwa.)

A. Findsecbugs

B. YASCA

C. Metasploit

D. theHarvester

E. Recon-ng

46. Które ustawienie zasad grupy systemu Windows określa, ile czasu musi upłynąć od nieudanej próby logowania, zanim licznik nieudanych prób logowania zostanie zresetowany do 0?

A. Czas trwania blokady konta

B. Próg blokady konta

C. Zresetuj licznik blokady konta po

D. Przechowuj hasła przy użyciu odwracalnego szyfrowania

47. Właśnie zakończyłeś test penetracyjny dla klienta, który korzysta z dużej liczby pracowników tymczasowych i wykonawców. W swoich ustaleniach informujesz, że konta użytkowników tymczasowych i kontraktowych często nie są dezaktywowane ani usuwane po zakończeniu ich prac. Biorąc pod uwagę, że komputery klienckie i serwery z systemem Linux, które z poniższych poleceń systemu Linux należy im zalecić, aby automatycznie blokować konta użytkowników po określonym czasie?

A. chage

B. chmod

C. chgroup

D. chown

48. Które z poniższych ustawień zasad grupy systemu Windows nigdy nie powinno być włączone?

A. Przechowuj hasła przy użyciu odwracalnego szyfrowania

B. Hasło musi spełniać wymagania dotyczące złożoności

C. Minimalna długość hasła

D. Ustawienia weryfikacji ścieżki certyfikatu path

E. Klient usług certyfikatów – automatyczne rejestrowanie

49. Podczas testu penetracyjnego odkrywasz, że Twój klient korzysta z aplikacji internetowej opracowanej we własnym zakresie, która przechowuje hasła użytkowników w postaci zwykłego tekstu w bazie danych MySQL. Co warto polecić?

A. Kup komercyjną aplikację, która wykonuje podobne zadanie.

B. Przepisz aplikację, aby szyfrować hasła przed ich zapisaniem w bazie danych.

C. Przejdź do bazy danych PostgreSQL.

D. Przejdź na rozwiązanie hostowane u dostawcy usług w chmurze.

50. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach informujesz, że chociaż użytkownicy są szkoleni w zakresie zmiany haseł co 45 dni, niewielu z nich faktycznie to robi, ponieważ nie ma mechanizmu egzekwowania tej polityki. Biorąc pod uwagę, że klient korzysta z komputerów stacjonarnych i serwerów z systemem Linux, którego z poniższych poleceń systemu Linux zaleca się użycie do automatycznego blokowania kont użytkowników, jeśli użytkownicy nie zmienią swoich haseł po 45 dniach?

A. chage

B. chmod

C. chgroup

D. chown

51. Sprzedawca internetowy bezpośrednio zajmuje się przetwarzaniem płatności za zamówienia kart kredytowych. W związku z tym firmy obsługujące karty kredytowe wymagają, aby organizacja była zgodna z PCIDSS. Kiedy ta organizacja musi przeprowadzić testy penetracyjne? (Wybierz dwa.)

A. Raz w miesiącu

B. Co sześć miesięcy

C. Raz w roku

D. Za każdym razem, gdy wprowadzane są znaczące zmiany w infrastrukturze sieciowej

E. Bezpośrednio przed szczytowymi sezonami sprzedaży, takimi jak święta

52. Robert pracuje dla firmy konsultingowej zajmującej się testami penetracyjnymi. Podczas niedawnego testu penetracyjnego uruchomił narzędzie do ataku na publicznie dostępną witrynę e-commerce klienta. Wyłączył się na ponad godzinę. Klient grozi teraz pozwaniem pracodawcy Roberta. Na jakim etapie procesu testów penetracyjnych firma doradcza i klient powinny uzgodnić ryzyka związane z testem?

A. Planowanie i ustalanie zakresu

B. Gromadzenie informacji i identyfikacja podatności

C. Atakowanie i wykorzystywanie

D. Raportowanie i komunikacja

53. Który z poniższych dokumentów jest dokumentem zdefiniowanym podczas fazy planowania i określania zakresu testu penetracyjnego, który identyfikuje konkretne techniki, narzędzia, czynności, produkty i harmonogramy testu?

A. MSA

B. Umowa o zachowaniu poufności

C. Protokół ustaleń

D. SOW

54. Który z poniższych rodzajów ocen zapewniłby testerowi penetracji dostęp do konfiguracji zapory sieciowej bez wymagania od testera faktycznego naruszenia zabezpieczeń zapory sieciowej?

A. Szare pudełko

B. Drużyna czerwona

C. Czarna skrzynka

D. Białe pudełko

55. Jesteś CIO startupu. Wybrałeś firmę przeprowadzającą testy penetracyjne, której chcesz użyć do przeprowadzenia pierwszego testu penetracyjnego firmy. Jednak założyciel firmy denerwuje się, gdy dowiaduje się o twoich planach. Założyciel obawia się, że zastrzeżone informacje o produktach firmy mogą wyciekać za pośrednictwem kontrahenta do konkurencji. O podpisanie jakiego dokumentu należy poprosić wykonawcę, aby temu zapobiec?

A. Umowa o zachowaniu poufności

B. Umowa o zakazie konkurencji

C. MSA

D. SOW

56. Robert przeprowadza test penetracyjny szarej skrzynki. Początkowo wyliczył sieć za pomocą testu ping i znalazł wewnętrzny serwer WWW, kontroler domeny, router i kilka urządzeń SCADA używanych na hali produkcyjnej. Które z tych urządzeń mogłoby potencjalnie zostać zakłócone przez bardziej intensywne skanowanie luk w zabezpieczeniach? (Wybierz dwa.)

A. Serwer WWW

B. Kontroler domeny

C. Router

D. Urządzenia SCADA

57. Robert przeprowadza test penetracyjny szarej skrzynki. Która z poniższych sytuacji będzie miała najmniejszy wpływ, kiedy będzie mógł przeprowadzić skanowanie podatności podczas testu?

A. Dostępność wewnętrznego personelu IT

B. Wymagania prawne

C. Ograniczenia sprzętowe

D. Szczytowe godziny ruchu w sieci organizacji

58. Robert przeprowadza test penetracji białej skrzynki. Organizacja docelowa w dużym stopniu opiera się na aplikacji opracowanej przez wewnętrznych programistów. Zakres testu określa, że ma on dostęp do kodu źródłowego tej aplikacji. Robert ma rozległe doświadczenie programistyczne, więc analizuje kod linia po linii w poszukiwaniu luk w zabezpieczeniach. Jaki rodzaj analizy aplikacji ma miejsce w tym scenariuszu?

A. Fuzzing

B. Statyczna analiza kodu

C. Dynamiczna analiza kodu

D. Analiza kodu heurystycznego

59. Robert przeprowadza test penetracji szarej skrzynki. Organizacja docelowa w dużym stopniu opiera się na aplikacji opracowanej przez wewnętrznych programistów. Uruchamia aplikację, a następnie używa narzędzia do wysyłania losowych, nieoczekiwanych danych do wejść aplikacji i analizuje, jak reaguje. Jaki rodzaj analizy aplikacji ma miejsce w tym scenariuszu?

A. Fuzzing

B. Statyczna analiza kodu

C. Analiza kodu heurystycznego

D. Analiza mutacji

60. Robert przeprowadza test penetracji białej skrzynki. Musi przeprowadzić inwazyjne skanowanie luk w zabezpieczeniach serwera bazy danych klientów docelowej organizacji. Co on powinien zrobić?

A. Uruchom skanowanie w systemie na żywo w godzinach szczytu.

B. Uruchom skanowanie około 9 rano w typowy dzień roboczy.

C. Najpierw uruchom skanowanie testowe w środowisku laboratoryjnym.

D. Pomiń skanowanie tego systemu.

61. Tester penetracyjny próbuje wykorzystać aplikację internetową używaną przez docelową organizację. Używa pola formularza w aplikacji internetowej, aby przesłać złośliwy plik wykonywalny na serwer sieciowy. Które z poniższych opisów opisują ten rodzaj exploita? (Wybierz dwa.)

A. Manipulacja plikami cookie

B. Katalog przekrojowy

C. Włączenie plików lokalnych

D. Skrypty między witrynami (XSS)

E. Zdalne włączenie pliku file

62. Które z poniższych są przykładami niezabezpieczonych praktyk kodowania?

A. Dołączanie komentarzy do kodu źródłowego

B. Sprawdzanie pól wejściowych pod kątem prawidłowo sformatowanych informacji

C. W tym podprogramy do obsługi warunków błędów

D. Cyfrowe podpisywanie kodu

E. Dostarczanie pełnych komunikatów o błędach

63. Które z poniższych są przykładami niezabezpieczonych praktyk kodowania?

A. Usuwanie komentarzy z kodu źródłowego przed wydaniem

B. Sprawdzanie pól wejściowych pod kątem prawidłowo sformatowanych informacji

C. Brak procedur obsługi błędów

D. Brak podpisywania kodu

E. Usuwanie nadmiernie pełnych komunikatów o błędach

64. Programista aplikacji internetowych umieścił nazwę użytkownika i hasło wymagane do uzyskania dostępu do instancji bazy danych w kodzie PHP aplikacji. To jest przykład jakich praktyk związanych z niezabezpieczonym kodem?

A. Komentarze w kodzie źródłowym

B. Warunki wyścigu

C. Nieuprawnione korzystanie z funkcji/niechronionych interfejsów API

D. Poświadczenia zakodowane na stałe

65. Twórca aplikacji internetowej umieścił następujący kod HTML na stronie formularza:

<typ wejścia=ukryty>

To jest przykład jakich praktyk związanych z niezabezpieczonym kodem?

A. Komentarze w kodzie źródłowym

B. Ukryte elementy

C. Nieuprawnione korzystanie z funkcji/niechronionych interfejsów API

D. Warunki wyścigu

66. Którego operatora relacyjnego można użyć zarówno w Bash, jak i PowerShell, aby sprawdzić, czy jedna wartość jest liczbowo mniejsza lub równa drugiej?

A. <=

B. -lt

C. -le

D. !<

67. Którego operatora relacyjnego można użyć zarówno w Pythonie, jak i Ruby, aby sprawdzić, czy jedna wartość jest liczbowo mniejsza lub równa drugiej?

A. <=

B. -lt

C. -le

D. !<

68. Musisz stworzyć skrypt Bash, aby uruchomić exploita przeciwko docelowej organizacji. W ramach skryptu musisz poprosić użytkownika o wprowadzenie wartości. Które polecenie zaakceptuje wartość wprowadzoną przez użytkownika i przypisze ją do zmiennej o nazwie TargetHost?

A. echo $TargetHost

B. read TargetHost

C. readln TargetHostH

D. input $TargetHost

69. W ramach testu penetracyjnego szarej skrzynki musisz utworzyć skrypt Bash, aby uruchomić exploita przeciwko docelowej organizacji. W ramach skryptu musisz wyświetlić na ekranie wartość zmiennej o nazwie TargetHost. Które polecenie to zrobi?

A. echo $TargetHost

B. write TargetHost

C. writeln TargetHost

D. output $TargetHost

70. Którego polecenia można użyć ze struktury sterowania przepływem if/then w skrypcie Bash, aby ocenić, czy określony warunek jest prawdziwy?

A. eval

B. ==

C. test

D. <>

71. W trakcie testu penetracyjnego tester musi komunikować się z klientem. Która z poniższych sytuacji spowodowałaby wystąpienie tej komunikacji? (Wybierz dwa.)

A. Po próbie testu system staje się niedostępny.

B. System pokazuje informację o wcześniejszym nieautoryzowanym dostępie.

C. System wykazuje brak pełnego utwardzenia.

D. Tester wykrył w systemie indywidualnie identyfikowalne dane.

E. Tester odkrywa coś, co znajduje się w systemie poza zakresem.

72. Tester penetracyjny przeprowadził ocenę bezpieczeństwa dla klienta. Raport wymienia łącznie dziewięć luk w zabezpieczeniach, z których cztery uznano za krytyczne. Klient nie ma budżetu na natychmiastowe naprawienie wszystkich luk. Co tester powinien zasugerować jako najlepszą opcję dla klienta w tych okolicznościach?

A. Zastosuj łatwe mechanizmy kompensacji krytycznych podatności, aby zminimalizować ryzyko, a następnie zmienić priorytety środków zaradczych.

B. Zidentyfikuj luki, które można najszybciej naprawić, i zajmij się nimi w pierwszej kolejności.

C. Najpierw zaimplementuj najmniej wpływający z krytycznych luk w zabezpieczeniach, a następnie usuń inne krytyczne luki w zabezpieczeniach.

D. Najpierw napraw najbardziej krytyczną lukę, nawet jeśli oznacza to, że naprawienie innych luk może zająć więcej czasu.

73. Penetracja przeprowadziła ocenę bezpieczeństwa klienta. Zauważono, że istnieje kilka portów o wysokim numerze nasłuchujących na publicznym serwerze sieciowym. Klient wskazuje, że używa tylko portu 443 dla aplikacji. Co tester powinien polecić klientowi?

A. Wyłącz niepotrzebne usługi.

B. Filtruj port 443 na określone adresy IP.

C. Zaimplementuj zaporę sieciową aplikacji internetowej.

D. Przeniesienie aplikacji do innego portu.

74. Jaka jest najlepsza rekomendacja dla klienta, aby złagodzić podatność, jeśli tester penetracyjny mógł wpisać polecenie SQL injection w polu tekstowym i uzyskać dostęp do informacji przechowywanych w bazie danych?

A. Zaimplementuj normalizację danych wejściowych.

B. Zainstaluj wykrywanie włamań oparte na hoście.

C. Wykonaj hartowanie systemu.

D. Losuj poświadczenia używane do logowania.

75. Tester penetracyjny przeprowadza test i po skompromitowaniu pojedynczej stacji roboczej tester jest w stanie manewrować w bok w całej domenie z bardzo małą liczbą przeszkód. Jakie strategie migracji powinny być zalecane do raportu dla klienta? (Wybierz trzy.)

A. Zastosuj dodatkową kontrolę dostępu do sieci.

B. W przypadku wszystkich logowań wymagaj uwierzytelniania wieloskładnikowego.

C. Dla każdego komputera wybierz losowo poświadczenia administratora lokalnego.

D. W przypadku administratorów lokalnych wyłącz logowanie zdalne.

E. Zwiększ wymagania dotyczące minimalnej złożoności hasła.

F. Umieść każdy host we własnej wirtualnej sieci lokalnej (VLAN).

G. Na każdej stacji roboczej włącz szyfrowanie całego dysku.

76. Jaka jest właściwa opcja polecenia do użycia z Android Debug Bridge (ADB), która umożliwia pobieranie plików z urządzenia z systemem Android?

A. download

B. copy

C. pull

D. push

77. Używając Drozera do przeprowadzenia oceny Androida dwóch oddzielnych aplikacji, które mają tego samego producenta, wykonujesz polecenie run app package.list, aby wyświetlić listę uprawnień aplikacji. Zauważasz w raporcie, że aplikacje mogą odczytywać i zapisywać pliki w pamięci zewnętrznej. Który komponent aplikacji chciałbyś przetestować pod kątem wad wtrysku?

A. Odbiorcy

B. Działania

C. Usługi

D. Dostawca treści

78. Python traktuje wszystko jako _____ i zmienne nie muszą być deklarowane przed ich użyciem.

A. Obiekt

B. Stała

C. Klasa

D. Metoda

79. Która opcja zapewnia właściwy sposób dziedziczenia klasy z modułu w Pythonie?

A. Z klasy importu modułu

B. Importuj klasę z modułu

C. Importuj klasę; moduł importu

D. Moduł importu; importuj klasę

80. Zespół Pentest przyszedł do ciebie i zapytał, co powinni zrobić z pozostałymi kopiami roboczymi raportu. Który dokument sugerowałbyś jako odniesienie dla zespołu do właściwych instrukcji obsługi raportów?

A. SOW

B. RoE

C. SLA

D. MSA