1. Atakujący pobiera z Internetu działo jonowe o niskiej orbicie, a następnie wykorzystuje je do przeprowadzenia ataku typu „odmowa usługi” na witrynę internetową byłego pracodawcy. Co to za napastnik?

A. Script kiddies

B. Haktywista

C. Przestępczość zorganizowana

D. Państwo narodowe

2. Atakujący przeprowadza atak na wykonawcę rządowego w sąsiednim kraju w celu uzyskania dostępu za pośrednictwem wykonawcy do rządowej infrastruktury sieciowej rywalizującego kraju. Atak kieruje i finansuje rząd kraju atakującego. Co to za zagrożenie?

A. Script kiddies

B. Haktywista

C. Przestępczość zorganizowana

D. Państwo narodowe

3. Grupa hakerów z krajów byłego bloku sowieckiego połączyła siły i udostępniła w Internecie aplikację ransomware. Ich celem jest wyłudzenie od swoich ofiar pieniędzy w postaci kryptowaluty. Co to za napastnik?

A. Złośliwy insider

B. Haktywista

C. Przestępczość zorganizowana

D. Państwo narodowe

4. Atakujący, który jest zagorzałym zwolennikiem solanek, atakuje i niszczy witrynę firmy, która zbiera krewetki solankowe i sprzedaje je jako pokarm dla ryb. Co to za napastnik?

A. Script kiddies

B. Haktywista

C. Przestępczość zorganizowana

D. Państwo narodowe

5. Pracownik właśnie otrzymał od swojego przełożonego bardzo negatywną ocenę wyników. Pracownik uważa, że recenzja była stronnicza, a niska ocena nieuzasadniona. W odwecie pracownik uzyskuje dostęp do poufnych informacji o wynagrodzeniach pracowników z serwera bazy danych HR i publikuje je anonimowo na Glassdoor. Co to za napastnik?

A. Script kiddies

B. Haktywista

C. Przestępczość zorganizowana

D. Złośliwy insider

6. Zostałeś zatrudniony do przeprowadzenia testu penetracyjnego czarnej skrzynki dla klienta. Chcesz użyć ataku typu spear phishing w celu ujawnienia poświadczeń uwierzytelniających używanych przez kluczowych pracowników organizacji. Jakich narzędzi lub technik możesz użyć, aby zebrać informacje potrzebne do przeprowadzenia tego ataku? (Wybierz dwa.)

A. Nurkowanie w śmietniku

B. theHarvester

C. skanowanie nmap

D. Skan Nessusa

E. Shodan

7. Zostałeś zatrudniony do przeprowadzenia testu penetracyjnego czarnej skrzynki dla klienta. Chcesz użyć ataku wielorybniczego, aby ujawnić dane uwierzytelniające używane przez kierownictwo organizacji. Jakich informacji możesz w tym celu użyć? (Wybierz dwa.)

A. Skan Nessusa

B. Komunikaty prasowe

C. Sonda Censys

D. Skanowanie OpenVAS

E. Wykonawczy bios

8. Które z poniższych kryteriów można uznać za OSINT związane z celem testu penetracyjnego? (Wybierz dwa.)

A. Posty w mediach społecznościowych

B. Wyniki skanowania nmap

C. Numery ubezpieczenia społecznego pracowników

D. Rozliczenia podatku od osób prawnych

E. Zeznania podatkowe od osób fizycznych kierownictwa wykonawczego

9. Które z poniższych można uznać za OSINT związane z celem testu penetracyjnego? (Wybierz dwa.)

A. Wyniki skanowania Nessusa

B. Informacje od testera penetracyjnego, który wpadł na jej drogę do siedziby organizacji

C. Informacje od rejestratora DNS organizacji

D. Oferty pracy na stronie internetowej organizacji

E. Informacje zebrane od niezadowolonego pracownika

10. Jesteś na etapie zbierania informacji w ramach testu penetracyjnego z wykorzystaniem czarnej skrzynki. Musisz określić zasięg organizacji docelowej, określając rodzaj używanej infrastruktury sieciowej. Które źródła OSINT mogą potencjalnie ujawnić te informacje? (Wybierz dwa.)

A. Oferty pracy na stronie internetowej organizacji

B. Skanowanie nmap sieci wewnętrznej

C. Skanowanie sieci wewnętrznej Nessusa

D. Informacje od testera penetracyjnego, który dotarł do siedziby organizacji

E. Życiorysy obecnych pracowników na LinkedIn

11. Zostałeś wynajęty do przeprowadzenia testu penetracyjnego czarnej skrzynki dla klienta. Kupujesz mały pendrive i ładujesz go złośliwym oprogramowaniem, które instaluje keylogger na komputerze ofiary i wysyła do Ciebie przechwycone informacje. Wchodzisz do drzwi wejściowych klienta i pytasz recepcjonistę o drogę do pobliskiego obiektu sportowego. Podczas rozmowy celowo upuszczasz dysk na podłogę, a następnie wychodzisz. Który exploit został wykorzystany w tym scenariuszu?

A. Surfowanie przez ramię

B. Upuszczenie klucza USB

C. Phishing

D. Pozyskiwanie

12. Który exploit wysyła e-maile bezkrytycznie do dużej liczby pracowników docelowej organizacji, przewidując, że pewien procent z nich kliknie szkodliwy odsyłacz zawarty w wiadomości?

A. Phishing

B. Spear phishing

C. Wyłudzanie wiadomości SMS

D. Whaling

13. Który exploit wykorzystuje wiadomości tekstowe do dostarczania wiadomości phishingowych?

A. Pozyskiwanie

B. Spear phishing

C. Wyłudzanie wiadomości SMS

D. Whaling

14. Który exploit wykorzystuje rozmowę telefoniczną, aby przekonać kogoś do ujawnienia poufnych informacji?

A. Vishing

B. Spear phishing

C. Phishing

D. Whaling

15. Które exploity wymagają od testera penetracji przeprowadzenia najpierw obszernego rozpoznania w celu zidentyfikowania konkretnych, wartościowych osób, które mogą być celem w organizacji? (Wybierz dwa.)

A. Spear phishing

B. Phishing

C. Upuszczenie klucza USB

D. Whaling

E. Wyłudzanie wiadomości SMS

16. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie TCP ACK hostów w sieci o adresach IP 192.168.1.10, 192.168.1.11 i 192.168.1.13. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.10-13 –sA

B. nmap 192.168.1.0/24 –sA

C. nmap 192.168.1.10/24 -sA

D. nmap 192.168.1.10-13 –sT

17. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Musisz użyć narzędzia nmap na swoim laptopie, aby uruchomić skanowanie UDP hostów w sieci o adresach IP 192.168.1.10, 192.168.1.11, 192.168.1.13 i 192.168.1.15. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.10-15 –sU

B. nmap 192.168.1.0/24 –sU

C. nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15-sU

D. nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15–U

18. Przeprowadzasz dla klienta test penetracyjny szarej skrzynki. Musisz użyć narzędzia nmap na swoim laptopie, aby wykryć wszystkie hosty w podsieci 192.168.1.0 (która używa maski podsieci 255.255.255.0) bez faktycznego skanowania portów na tych hostach. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.0/16 –sL

B. nmap 192.168.1.1-254 -sn

C. nmap 192.168.1.1-254 -sW

D. nmap 192.168.1.0/16 -sM

19. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Musisz użyć narzędzia nmap na swoim laptopie, aby wykryć wszystkie hosty w podsieci 192.168.1.0 (która używa maski podsieci 255.255.255.0), które mają otwarty port Telnet. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.0/24 – s 23

B. nmap 192.168.1.0/24 –p 21

C. nmap 192.168.1.1-254 –p 21

D. nmap 192.168.1.1-254 –p 23

20. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Musisz użyć narzędzia nmap na swoim laptopie, aby przeskanować wszystkie porty na hoście sieciowym o adresie IP 192.168.1.2. Którego polecenia powinieneś użyć, aby to zrobić?

A. nmap 192.168.1.2 -p

B. nmap 192.168.1.2 –p all

C. nmap 192.168.1.2 –s wszystko

D. nmap 192.168.1.2 –p 1-1024

21. Podczas testu penetracyjnego dana osoba zostaje przyłapana na próbie wpięcia się do obiektu organizacji klienta. Intruz twierdzi, że jest testerem penetracji i nalega na uwolnienie. Przed wniesieniem zarzutów karnych członek personelu IT klienta dzwoni do testera penetracyjnego, aby ustalić, czy intruz rzeczywiście jest członkiem zespołu testów penetracyjnych. Jak nazywa się ta ścieżka komunikacji?

A. Zmiana priorytetów celów

B. Konflikt

C. Świadomość sytuacyjna

D. Deeskalacja

22. Podczas testu penetracyjnego tester uzyskuje fizyczny dostęp do obiektu klienta za pomocą pretekstu i jest w stanie wywołać zdarzenie awaryjne dla wszystkich elektronicznych systemów zamknięć organizacji. Dzięki temu wszystkie drzwi w placówce zostają odblokowane. Wewnętrzny zespół bezpieczeństwa klienta dzwoni do testera penetracji i prosi o zatrzymanie ataku i natychmiastowe ponowne włączenie zamków w drzwiach. Jak nazywa się ten proces?

A. Świadomość sytuacyjna

B. Zmiana priorytetów celów

C. Dekonflikt

D. Deeskalacja

23. Które z poniższych stwierdzeń najlepiej opisuje zaufanego agenta podczas testu penetracyjnego?

A. Tester, który potajemnie penetruje organizację docelową, starając się tam o pracę

B. Osoba w organizacji docelowej, która ma bezpośrednią linię komunikacji z testerem penetracyjnym

C. Osoba w zespole ds. testów penetracyjnych, która ma bezpośrednią linię komunikacji z personelem IT organizacji docelowej

D. Przedstawiciel lokalnego organu ścigania, który został poinformowany o teście przez penetratora testera

24. Przeprowadzasz test penetracyjny czarnej skrzynki dla klienta.

Faza rekonesansu testu dobiegła końca i jesteś gotowy, aby przejść do następnej fazy. Zanim to zrobisz, komunikujesz się z klientem i informujesz go, że test przechodzi z jednej fazy do drugiej. 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 szarej skrzynki dla klienta. Podczas testu odkrywasz, że komputerowe systemy Windows wielu użytkowników nie zostały odpowiednio załatane i nadal są podatne na kilka popularnych typów oprogramowania ransomware. Zamiast czekać do końca testu, natychmiast komunikujesz się z klientem, aby ostrzec go, że jego systemy są podatne na ataki. Jaki typ wyzwalacza komunikacji został użyty w tym scenariuszu?

A. Ocena ryzyka

B. Krytyczne ustalenia

C. Ustalenia i środki zaradcze

D. Wskaźniki wcześniejszego kompromisu

26. Klient poprosił Cię o przeprowadzenie testu penetracyjnego białej skrzynki. Celem jest ocena bezpieczeństwa ich aplikacji internetowych. Te aplikacje są oparte na architekturze Representational State Transfer (REST). Podczas procesu określania zakresu stwierdzasz, że pomocne byłoby, gdybyś miał dostęp do wewnętrznej dokumentacji organizacji dla tych aplikacji. O które z poniższych pytań powinieneś zapytać swojego klienta?

A. Dokumentacja języka opisu usług sieciowych (WSDL)

B. Dokumentacja zestawu programistycznego (SDK)

C. Dokumentacja języka opisu aplikacji internetowych (WADL)

D. Dokumentacja interfejsu programowania aplikacji (API)

27. Klient poprosił Cię o przeprowadzenie testu penetracyjnego białej skrzynki. Celem jest ocena bezpieczeństwa kilku aplikacji na komputery PC, które zostały napisane we własnym zakresie przy użyciu języka programowania C++. Aplikacje te są używane na co dzień przez pracowników do zarządzania zamówieniami, zapasami i wypłatami. Podczas procesu określania zakresu ustalasz, że byłoby pomocne, gdybyś miał dostęp do wewnętrznej dokumentacji rozwoju oprogramowania organizacji dla tych aplikacji. O które z poniższych pytań powinieneś zapytać swojego klienta? (Wybierz dwa.)

A. Dokumentacja protokołu SOAP (Simple Object Access Protocol)

B. Dokumentacja zestawu programistycznego (SDK)

C. Dokumentacja języka opisu aplikacji internetowych (WADL)

D. Dokumentacja interfejsu programowania aplikacji (API)

28. Przygotowujesz dla klienta test penetracyjny z czarną skrzynką. Celem jest sprawdzenie, czy możesz uzyskać dostęp do informacji przechowywanych na wewnętrznym serwerze bazy danych. Jakie informacje powinien udzielić Ci klient przed rozpoczęciem testu?

A. Schematy architektoniczne

B. Dokument Swagger

C. XSD

D. Schematy sieciowe

29. Przygotowujesz test penetracyjny białej skrzynki dla klienta. Celem jest sprawdzenie, czy możesz uzyskać dostęp do poufnych danych badawczych przechowywanych na wewnętrznym serwerze bazy danych. Celem jest stworzenie wewnętrznie opracowanej aplikacji do gromadzenia danych, której użytkownicy końcowi klienta używają na co dzień do katalogowania i przechowywania informacji w bazie danych. Jakie informacje powinien udzielić Ci klient przed rozpoczęciem testu?

A. Schematy architektoniczne

B. Przykładowe prośby

C. XSD

D. Wszystkie powyższe

30. Sprawdzasz dla klienta test penetracyjny białej skrzynki. Celem jest sprawdzenie, czy możesz uzyskać dostęp do poufnych danych klientów przechowywanych na wewnętrznym serwerze bazy danych. Poprosiłeś klienta o schematy architektoniczne. Jakie informacje powinien Ci udzielić klient? (Wybierz dwa.)

A. Dokument Swagger

B. Dokumentacja protokołu SOAP (Simple Object Access Protocol)

C. Schematy sieciowe

D. XSD

E. Mapy obiektów

31. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Pracownicy w organizacji docelowej korzystają z aplikacji opracowanej we własnym zakresie, aby wykonywać swoją codzienną pracę. Często się zawiesza i podejrzewasz, że jest oparty na źle napisanym lub nieaktualnym kodzie. Chcesz przeanalizować kod źródłowy aplikacji, aby sprawdzić, czy zawiera słabości, które można wykorzystać. Jednak zasady zaangażowania w test nie pozwalają na dostęp do kodu. Co powinieneś zrobić?

A. Zdekompiluj plik wykonywalny aplikacji.

B. Debuguj plik wykonywalny aplikacji.

C. Przechwytuj i analizuj ruch sieciowy generowany przez aplikację podczas korzystania z niej przez pracowników.

D. Nadaj priorytet ruchowi sieciowemu generowanemu przez aplikację przy użyciu ustawień jakości usług (Qos) na przełączniku.

32. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Chcesz kierować aplikację na wewnętrzną aplikację, z której codziennie korzystają pracownicy organizacji. Aby zidentyfikować słabe punkty w kodzie, decydujesz się na dekompilację pliku wykonywalnego aplikacji. Masz pewne doświadczenie w programowaniu w C++, więc możesz swobodnie przeglądać kod źródłowy ujawniony

w procesie dekompilacji. Jednak po dekompilacji okazuje się, że nie rozumiesz zawartości utworzonego pliku kodu źródłowego. Dlaczego się to stało?

A. Musisz przekonwertować dane wyjściowe do C++.

B. Dekompilatory zwykle tworzą kod na poziomie asemblera.

C. Zapomniałeś użyć opcji –C podczas uruchamiania dekompilatora.

D. Aplikacja jest tak źle napisana, że dekompilator nie jest w stanie odtworzyć kodu źródłowego.

33. Przeprowadzasz test penetracyjny szarej skrzynki dla klienta. Pracownicy w organizacji docelowej korzystają z aplikacji opracowanej we własnym zakresie, aby wykonywać swoją codzienną pracę. Często się zawiesza i podejrzewasz, że jest oparty na źle napisanym lub nieaktualnym kodzie. Chcesz przeanalizować działanie aplikacji uruchamianej przez typowego użytkownika końcowego, aby sprawdzić, czy zawiera ona słabości, które można wykorzystać. Co powinieneś zrobić?

A. Zdekompiluj plik wykonywalny aplikacji.

B. Debuguj plik wykonywalny aplikacji.

C. Przechwytuj i analizuj ruch sieciowy generowany przez aplikację podczas korzystania z niej przez pracowników.

D. Nadaj priorytet ruchowi sieciowemu generowanemu przez aplikację przy użyciu ustawień jakości usług (Qos) na przełączniku.

34. Które źródło badań typu open source jest utrzymywane przez rząd USA i zapewnia dynamiczne podsumowanie najczęściej zgłaszanych rodzajów incydentów bezpieczeństwa o dużym wpływie?

A. CERT

B. JPCERT

C. CVE

D. CAPEC

35. Które źródło badań typu open source jest utrzymywane przez rząd japoński i zapewnia dynamiczne podsumowanie bieżących ostrzeżeń i porad dotyczących bezpieczeństwa?

A. CERT

B. JPCERT

C. CWE

D. CAPEC

36. Które z poniższych exploitów są wspierane przez słabości protokołu SMB? (Wybierz dwa.)

A. Distributed denial of service (DDoS)

B. Fraggle

C. Teardrop

D. EternalBlue

E. WannaCry y

37. Jakie porty są używane przez protokół SMB? (Wybierz dwa.)

A. 53

B. 80

C. 139

D. 443

E. 445

38. Które z poniższych są lukami związanymi z protokołem SNMPv1? (Wybierz dwa.)

A. Ciąg wspólnoty jest prawidłowy dla każdego węzła SNMPv1.

B. Ciąg społeczności jest przesyłany w postaci zwykłego tekstu.

C. Łańcuch wspólnoty używa słabego szyfru RC2.

D. Do komunikacji z hostem SNMPv1 nie jest wymagane uwierzytelnianie.

E. Baza informacji zarządzania (MIB) jest przechowywana w formacie niezaszyfrowanym.

39. Który port jest używany przez protokół SNMP?

A. UDP 161

B. TCP 23

C. TCP 389

D. UDP 88

40. Jaka jest funkcja Simple Mail Transfer Protocol (SMTP)?

A. Udostępnianie plików w sieci

B. Przesyłanie wiadomości e-mail między agentami przesyłania poczty (MTA)

C. Mapowanie adresów IP na adresy MAC

D. Przesyłanie wiadomości e-mail do agenta użytkownika poczty (MUA)

41. Jakie narzędzie jest używane do przeprowadzania exploitów socjotechnicznych?

A. Responder

B. SET

C. APKX

D. Immunity debugger

E. Hopper

42. Które narzędzie do testowania penetracji koncentruje się na wykorzystywaniu przeglądarek internetowych?

A. BeEF

B. foremost

C. FTK

D. EnCase

E. Tableau

43. W ramach testu penetracyjnego chcesz uzyskać dostęp do sesji powłoki na docelowym serwerze Windows. Jakiego narzędzia można do tego użyć?

A. Ollydbg

B. GDB

C. WinDBG

D. ncat

44. W ramach testu penetracyjnego chcesz odwrócić kompilację pliku wykonywalnego dla opracowanej wewnętrznie aplikacji używanej przez organizację docelową. Które z poniższych narzędzi można do tego wykorzystać? (Wybierz dwa.)

A. IDA

B. Hopper

C. route

D. Tableau

E. FTK

45. Które z poniższych narzędzi są wykorzystywane do zbierania i analizowania dowodów z cyfrowego miejsca przestępstwa? (Wybierz dwa.)

A. APKX

B. Peach

C. foremost

D. AFL

E. FTK

46. Które z poniższych ustawień zasad grupy systemu Windows określa, jak długo użytkownik może przechowywać to samo hasło, zanim będzie musiał zmienić je na nowe?

A. Wymuszaj historię haseł

B. Minimalna długość hasła

C. Minimalny wiek hasła

D. Maksymalny wiek hasła

47. Które z poniższych ustawień zasad grupy systemu Windows określa, jak długo użytkownik musi przechowywać to samo hasło, zanim będzie mógł je zmienić na nowe?

A. Wymuszaj historię haseł

B. Minimalna długość hasła

C. Minimalny wiek hasła

D. Maksymalny wiek hasła

48. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach zgłaszasz, że użytkownicy mogą przechowywać to samo hasło bezterminowo, co zwiększa prawdopodobieństwo, że w pewnym momencie zostaną naruszeni. Biorąc pod uwagę, że klient korzysta z komputerów stacjonarnych i serwerów z systemem Linux, którego z poniższych poleceń systemu Linux należy im polecić, aby rozwiązać ten problem?

A. chage

B. chmod

C. chgroup

D. chown

49. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach informujesz, że ataki brute-force na hasła na konta użytkowników w domenie Windows zakończyły się sukcesem, ponieważ nic nie powstrzymało oprogramowania do łamania haseł przed próbowaniem kolejnych haseł dla danego użytkownika. Które z następujących ustawień zasad grupy domeny systemu Windows można zalecić klientowi zaimplementowanie w celu rozwiązania tego problemu?

A. Wymuszaj historię haseł

B. Hasło musi spełniać wymagania dotyczące złożoności

C. Przechowuj hasła przy użyciu odwracalnego szyfrowania

D. Próg blokady konta

50. Które ustawienie zasad grupy systemu Windows określa, jak długo konto użytkownika pozostanie zablokowane, jeśli nieprawidłowe hasło zostanie wprowadzone zbyt wiele razy?

A. Maksymalny wiek hasła

B. Czas trwania blokady konta

C. Próg blokady konta

D. Minimalny wiek hasła

51. Które z poniższych najlepiej opisuje termin odmowa w kontekście testów penetracyjnych?

A. Uzyskanie nieautoryzowanego dostępu do informacji

B. Dokonywanie nieautoryzowanych zmian w informacjach

C. Zapobieganie zgodnemu z prawem wykorzystaniu informacji

D. Brak publicznego potwierdzenia, że doszło do naruszenia bezpieczeństwa i że informacje zostały naruszone

52. Robert przeprowadza test penetracyjny szarej skrzynki i odkrywa lukę w aplikacji internetowej, która umożliwia mu bezpośredni dostęp do informacji przechowywanych na serwerze bazy danych zaplecza. Jaki cel testów penetracyjnych osiągnął?

A. Ujawnienie

B. Uczciwość

C. Zmiana

D. Odmowa

53. Robert przeprowadza test penetracyjny szarej skrzynki i odkrywa lukę w internetowej aplikacji katalogu firmowego, która umożliwia mu przesyłanie poleceń LDAP w polu wyszukiwania pracowników. Wykorzystuje tę lukę, aby dodać nowe konto użytkownika, które może wykorzystać jako tylne drzwi. Jaki cel testów penetracyjnych osiągnął?

A. Ujawnienie

B. Dostępność

C. Zmiana

D. Odmowa

54. Robert przeprowadza test penetracji szarej skrzynki. Używa narzędzia Low Orbit Ion Cannon do wysyłania powodzi pakietów TCP do serwera plików w organizacji. W rezultacie serwer plików staje się przeciążony i nie może już odpowiadać na uzasadnione żądania sieciowe. Jaki cel testów penetracyjnych osiągnął?

A. Ujawnienie

B. Poufność

C. Zmiana

D. Odmowa

55. Robert przeprowadza test penetracyjny szarej skrzynki. Odkrywa lukę w internetowej aplikacji HR. Za pomocą ataku SQL injection może dodawać lub usuwać godziny do lub z karty czasowej pracownika w bieżącym okresie rozliczeniowym. Jaki cel testów penetracyjnych osiągnął?

A. Ujawnienie

B. Dostępność

C. Zmiana

D. Poufność

56. Podczas testu penetracji szarej skrzynki uruchamiasz skanowanie nmap systemu wykrytego w sieci. Okazuje się, że porty TCP 139, 443 i 3389 są otwarte. Jaki system operacyjny najprawdopodobniej działa w systemie?

A. iOS

B. Windows

C. Linux

D. Android

57. Przeprowadzasz test penetracji szarej skrzynki. Uruchamiasz skanowanie pod kątem luk w zabezpieczeniach hosta i stwierdzasz, że porty TCP 8080 i 8443 są otwarte. Co możesz wywnioskować o tym hoście z tych informacji?

A. Prawdopodobnie jest to serwer DNS.

B. Jest to prawdopodobnie kontroler domeny.

C. Jest to prawdopodobnie serwer plików.

D. Jest to prawdopodobnie serwer WWW.

58. Robert przeprowadza test penetracji szarej skrzynki. Sieć docelowa używa 10-netowego schematu adresowania IP z 8-bitową maską podsieci (10.0.0.0/8). Musi przeprowadzić skanowanie podatności na każdym hoście w sieci. Ładuje nmap na swoim laptopie, który jest podłączony do tego samego segmentu, który jest skanowany, używając opcji - T0. Co zrobił niepoprawnie w tym scenariuszu?

A. Narzędzie nmap nie działa z prywatnymi schematami adresowania IP.

B. Narzędzie nmap powinno być uruchamiane z hosta, który nie jest podłączony do tego samego skanowanego segmentu.

C. Opcja -T0 spowoduje, że skanowanie w tak dużej podsieci zajmie bardzo dużo czasu.

D. Szybkość skanowania można zwiększyć, używając komputera stacjonarnego zamiast laptopa.

59. Robert przeprowadza test penetracji czarnej skrzynki. Musi dowiedzieć się, kto jest rejestratorem domeny organizacji docelowej. Chciałby też poznać adres i numer telefonu organizacji. Jakiego narzędzia powinien użyć?

A. whois

B. TheHarvester

C. dig

D. nslookup

60. Robert przeprowadza test penetracji czarnej skrzynki. Chce przeprowadzić skanowanie podatności sieci wewnętrznej organizacji docelowej. Co on powinien zrobić?

O. Poproś organizację docelową o pozwolenie na przybycie na miejsce i przeprowadzenie skanowania.

B. Poproś, aby organizacja docelowa przyznała mu dostęp VPN do sieci wewnętrznej.

C. Spróbuj skompromitować hosta wewnętrznego i użyj go jako punktu obrotu.

D. Uruchom skanowanie zewnętrznie.

61. Jakie formy ataku typu cross-site scripting (XSS) są uważane za exploity po stronie serwera? (Wybierz dwa.)

A. Przechowywane/trwałe

B. Odbiie

C. Obiektowy model dokumentu (DOM)

D. Clickjacking

E. Katalog przekrojowy

62. Podczas testu penetracyjnego w szarej strefie tester zauważa, że samoobsługowa aplikacja sieciowa do obsługi zasobów ludzkich organizacji używa kont użytkowników Active Directory do uwierzytelniania. Zawiera również opcję „Zapamiętaj mnie" na stronie logowania. Tester wysyła wiadomość e-mail do pracowników wysokiego szczebla w organizacji z tematem „Sprawdź to zabawne zdjęcie". Po otwarciu wiadomości e-mail ukryty kod HTML faktycznie wysyła żądanie HTTP do samoobsługowej aplikacji internetowej, która zmienia hasło użytkownika. Atak opiera się na zapisanym sesyjnym pliku cookie z witryny do działania. Jaki to rodzaj exploita uwierzytelniania?

A. Skrypty między witrynami (XSS)

B. Fałszowanie żądań między witrynami (CSRF)

C. Clickjacking

D. brutalne wymuszanie uwierzytelnienia

63. Który exploit uwierzytelniania wykorzystuje przezroczyste warstwy na tej samej stronie internetowej, aby nakłonić użytkownika do kliknięcia przycisku lub łącza, gdy myślał, że po prostu klika warstwę najwyższego poziomu strony?

A. Włączenie pliku

B. Fałszowanie żądań między witrynami (CSRF)

C. Clickjacking

D. Manipulacja plikami cookie

64. Która błędna konfiguracja zabezpieczeń na serwerze sieciowym pozwoliłaby użytkownikowi końcowemu uzyskującemu dostęp do witryny za pomocą przeglądarki internetowej na poruszanie się po systemie plików serwera internetowego?

A. Katalog przekrojowy

B. Manipulacja plikami cookie

C. Włączenie pliku

D. Słabe referencje

65. Która błędna konfiguracja zabezpieczeń pozwoliłaby skryptowi uruchamianemu przez przeglądarkę internetową użytkownika na zapisanie danych w pliku cookie po stronie klienta?

A. Katalog przekrojowy

B. Manipulacja plikami cookie

C. Fałszowanie żądań między witrynami (XSRF)

D. Clickjacking

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

A. >=

B. -gt

C. -ge

D. !>=

67. Którego operatora relacyjnego można użyć zarówno w Bash, jak i PowerShell, aby sprawdzić, czy jedna wartość jest liczbowo większa od drugiej?

A. >=

B. -gt

C. -ge

D. !>=

68. Którego operatora relacji można użyć zarówno w Pythonie, jak i Ruby, aby sprawdzić, czy jedna wartość jest liczbowo większa lub równa drugiej?

A. >=

B. -gt

C. -ge

D. !>=

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

A. <=

B. -lt

C. -le

D. !<

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

A. <=

B. -lt

C. -le

D. <

71. Spotykasz się ze swoim klientem po zakończeniu testu penetracyjnego. Podczas spotkania przekazujesz klientowi szczegółowe dowody związane z problemami, które odkryłeś podczas testu. Jak nazywa się ten proces?

A. Poświadczenie ustaleń

B. Wyciągnięte wnioski

C. Akceptacja klienta

D. Normalizacja danych

72. Spotykasz się ze swoim klientem po zakończeniu testu penetracyjnego. Na zakończenie spotkania prosisz klienta o pisemne potwierdzenie, że wypełniłeś swoje obowiązki zgodnie z umową, którą pierwotnie podpisano z klientem. Jak nazywa się ten proces?

A. Poświadczenie ustaleń

B. Wyciągnięte wnioski

C. Akceptacja klienta

D. Działania następcze

73. Kilka miesięcy po zakończeniu testu penetracyjnego Twój klient dzwoni i prosi Cię o powrót i ponowne przetestowanie jego sieci w celu sprawdzenia, czy wykryte przez Ciebie problemy zostały odpowiednio naprawione. Jak nazywa się ten proces?

A. Poświadczenie ustaleń

B. Wyciągnięte wnioski

C. Działania następcze

D. Normalizacja danych

74. Po zakończeniu testu penetracyjnego dla klienta spotykasz się z zespołem ds. testów penetracyjnych, aby przejrzeć wyciągnięte wnioski. Co powinieneś zrobić na tym spotkaniu? (Wybierz dwa.)

A. Udokumentuj techniczne exploity, które były skuteczne podczas testu.

B. Omów najlepsze miejsca do jedzenia w pobliżu lokalizacji klienta.

C. Zidentyfikuj exploity, które nie były skuteczne podczas testu.

D. Przejrzyj plany swojego zespołu na nadchodzące obchody świąt.

75. Analitykowi bezpieczeństwa przekazano szczegółowy raport dotyczący penetracji. Penetracja została przeprowadzona przeciwko środowisku DMZ organizacji docelowej. W raporcie stwierdzono, że system punktowej oceny podatności na zagrożenia (CVSS) ma bazowy wynik 1,0. Aby wykorzystać tę lukę, jaki poziom trudności byłby wymagany?

O. Bardzo trudne, ponieważ systemy obwodowe są zwykle za zaporą ogniową

B. Trochę trudne, ponieważ wykorzystanie tego wymagałoby potężnego przetwarzania

C. Trywialne, ponieważ wykorzystanie wyników wymagałoby niewielkiego wysiłku

D. Niemożliwe, ponieważ zewnętrzne hosty są zabezpieczone przed atakami

76. Podczas pentestu natrafiasz na prywatny klucz SSH (id_rsa) w katalogu domowym użytkownika i podejrzewasz, że ten klucz może być użyty do zdalnego logowania się do innych hostów Linux. Jednak zanim spróbujesz użyć klucza, chcesz porównać klucz z zawartością pliku authorize_keys, aby upewnić

się, że pasuje do jednego z kluczy publicznych przechowywanych w pliku. Jakie polecenie uruchomisz, aby wygenerować klucz publiczny z klucza prywatnego?

A. ssh-keygen -y -f id_rsa

B. ssh-keygen -t rsa -b 2048

C. diff id_rsa.pub id_rsa

D. openssl rsa -in id_rsa | kot id_rsa.pub

77. Pistolet pick-up emuluje jaki rodzaj ruchu otwierania zamków?

A. Raking

B. SPP

C. Jiggling

D. Scrubbing

78. Styropian to rodzaj izolatora, który jest dobry w pokonaniu jakiego rodzaju czujnika?

A. Ultradźwiękowy

B. Magnetyczne

C. Podczerwień

D. Kuchenka mikrofalowa

79. Niektóre rodzaje zamków szyfrowych można pokonać za pomocą jakiego typu narzędzia omijania, które wymaga niewiele wysiłku do wykonania i jest rozsądne z punktu widzenia medycyny sądowej?

A. Magnes

B. Śrubokręt

C. Młot

D. Brutalna siła

80. Jakie polecenie należy wpisać w konsoli Metasploit, aby zabić wszystkie aktywne sesje ze zdalnymi celami?

A. sessions -k

B. sessions -K

C. kill -9

D. kill sessions