1. Pracujesz w firmie konsultingowej zajmującej się testami penetracyjnymi. Organizacja, z którą wcześniej nie współpracowałeś, dzwoni i prosi o wykonanie czarnej skrzynki oceny jej sieci. Ustalasz cenę i zakres przez telefon. Po szybkim zaprojektowaniu testu na papierze, zaczynasz wykonywanie później tego samego popołudnia. Czy ten test został przeprowadzony prawidłowo?

A. Tak, przestrzegano właściwych procedur planowania i określania zakresu testów penetracyjnych.

B. Nie, nowi klienci powinni zostać odpowiednio zweryfikowani przed rozpoczęciem oceny.

C. Nie, przed rozpoczęciem testowania należy podpisać główną umowę serwisową (MSA).

D. Nie, zasady zaangażowania (ROE) do testu powinny być udokumentowane i podpisane przez obie strony.

2. Umawiasz się z nowym klientem na przeprowadzenie testu penetracyjnego. Która z poniższych opcji jest odpowiednim sposobem uzyskania prawnego pozwolenia na przeprowadzenie testu?

A. Poproś członka kierownictwa wyższego szczebla za pośrednictwem poczty elektronicznej o zgodę na wykonanie testu.

B. Poproś pracownika działu IT przez telefon o zgodę na wykonanie testu.

C. Poproś członka personelu IT o podpisanie dokumentu uprawniającego do wykonania testu.

D. Poproś członka kierownictwa wyższego szczebla o podpisanie dokumentu uprawniającego do wykonania testu.

3. Który rodzaj testu penetracyjnego najlepiej symuluje atak z zewnątrz?

A. Black box

B. Gray box

C. White box

D. Blue box

4. Musisz przeprowadzić test penetracyjny dla klienta, który najlepiej oceni podatność organizacji docelowej na złośliwego insidera, który ma uprawnienia sieciowe przeciętnego pracownika. Jaki rodzaj testu powinieneś wykonać?

A. Gray box

B. White box

C. Black box

D. Red box

5. Jaki rodzaj testu penetracyjnego wymaga najwięcej czasu i pieniędzy?

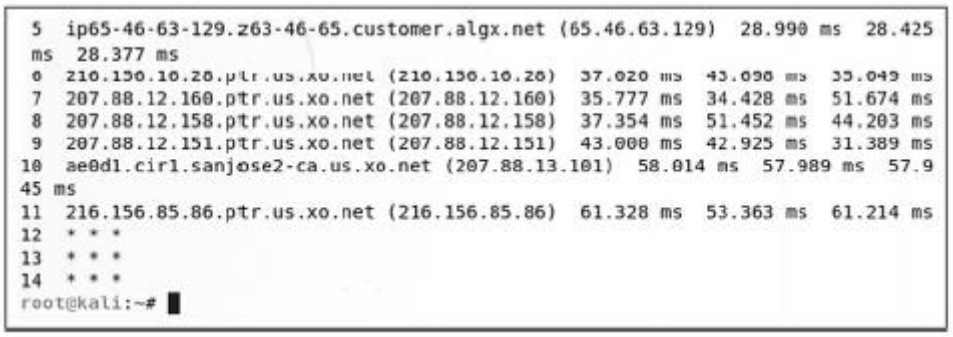
A. White box

B. Gray box

C. Black box

D. Green box

6. Podczas fazy wykrywania testu penetracji czarnej skrzynki uruchamiasz polecenie traceroute, aby wykryć trasę przez Internet do serwera WWW organizacji docelowej. Wyniki są pokazane tutaj:



Co oznaczają znaki *** w liniach 12, 13 i 14?

A. Powiązane urządzenia zostały skonfigurowane tak, aby nie odpowiadały na pingi.

B. Nazwy hostów powiązanych urządzeń nie mogły zostać rozpoznane przez serwer DNS.

C. Powiązane urządzenia nie działają.

D. Twój komputer został umieszczony na czarnej liście tych urządzeń na trasie.

7. Podczas fazy wykrywania testu penetracyjnego czarnej skrzynki korzystasz ze strony centralops.net, aby przeprowadzić rozpoznanie nazwy domeny docelowej organizacji. Częściowe wyniki są pokazane tutaj:

Jakie usługi publiczne są dostępne dla tej nazwy domeny? (Wybierz dwa.)

A. FTP

B. Bezpieczna poczta e-mail

C. Niebezpieczny serwer WWW

D. Bezpieczny serwer WWW

E. Niepewny e-mail

F. Bezpieczna powłoka

8. Podczas fazy wykrywania w teście penetracji czarnej skrzynki korzystasz ze strony centralops.net, aby przeprowadzić rozpoznanie nazwy domeny docelowej organizacji. Częściowe wyniki są pokazane tutaj:

Które z poniższych są prawdziwe? (Wybierz dwa.)

A. Certyfikat organizacji wygasł w 2017 roku.

B. SHA1 został użyty do podpisania certyfikatu organizacji.

C. Organizacja korzysta z serwera WWW Apache.

D. SHA256 został użyty do podpisania certyfikatu organizacji.

E. Serwer sieciowy organizacji działa w systemie Windows.

9. Podczas fazy wykrywania testu penetracyjnego wykorzystującego czarną skrzynkę zidentyfikowałeś adres e-mail, który, jak podejrzewasz, należy do kierownictwa w organizacji docelowej. Korzystasz ze strony centralops.net, aby przeanalizować ten adres e-mail. Wyniki są pokazane tutaj:

Czego możesz się nauczyć z wyników?

A. To jest prawidłowy adres e-mail.

B. To jest nieprawidłowy adres e-mail.

C. Ten adres e-mail należy do danego dyrektora.

D. Ten adres e-mail należy do pracownika działu pomocy.

10. W fazie odkrywania testu penetracyjnego wykorzystującego czarną skrzynkę zidentyfikowałeś adres e-mail, który podejrzewasz, że należy do kierownictwa w organizacji docelowej. Korzystasz ze strony centralops.net, aby przeanalizować ten adres e-mail. Wyniki są pokazane tutaj:

Czego możesz się nauczyć z wyników?

A. Serwer poczty e-mail organizacji ma adres IP 208.101.20.81.

B. Konwencja nazewnictwa adresów e-mail organizacji to

first_initial+lastname@company_name.com.

C. Konwencja nazewnictwa adresów e-mail organizacji to first_initial.lastname@company_name.com.

D. Serwer poczty e-mail organizacji nie odpowiada na polecenia HELO.

11. Jaki czynnik motywacyjny skłania ludzi do szybkiego działania z powodu poczucia ograniczonej podaży?

A. Dowód społeczny

B. Podobieństwo

C. Niedobór

D. Władza

12. Jaki czynnik motywacyjny skłania ludzi do działania, ponieważ wierzą, że „wszyscy to robią”?

A. Dowód społeczny

B. Strach

C. Niedobór

D. Władza

13. Jaki czynnik motywacyjny skłania ludzi do działania, ponieważ chce tego ktoś o dużej sile przebicia?

A. Podobieństwo

B. Dowód społeczny

C. Władza

D. Niedobór

14. Jaki czynnik motywacyjny skłania ludzi do szybkiego działania, ponieważ uważają, że ktoś potrzebuje pomocy?

A. Dowód społeczny

B. Pośpiech

C. Niedobór

D. Władza

15. Jaki czynnik motywacyjny skłania ludzi do działania, ponieważ chcą zadowolić osobę, która o nich prosi?

A. Podobieństwo

B. Dowód społeczny

C. Władza

D. Niedobór

16. Która opcja taktowania nmapa powoduje skanowanie w trybie Polite?

A. -T0

B. -T1

C. -T2

D. -T3

E. -T4

17. Która opcja powoduje, że nmap zapisuje swoje dane wyjściowe do standardowego pliku tekstowego w systemie plików hosta, na którym został uruchomiony?

A. -oX

B. -oN

C. -oT

D. -oV

18. Która opcja powoduje, że nmap zapisuje swoje dane wyjściowe do pliku tekstowego w formacie XML w systemie plików hosta, na którym został uruchomiony?

A. -oX

B. -oN

C. -oT

D. -oG

19. Która opcja powoduje, że nmap zapisuje swoje dane wyjściowe do pliku tekstowego, który można szybko przeszukać za pomocą polecenia grep?

A. -oV

B. -oN

C. -oT

D. -oG

20. Która opcja powoduje, że nmap zapisuje swoje dane wyjściowe w normalnym pliku tekstowym, w pliku tekstowym w formacie XML oraz w pliku tekstowym z możliwością grppowania?

A. -oX

B. -oN

C. -oA

D. –oG

21. Generujesz pisemny raport ustaleń po teście penetracyjnym. Podczas testu odkryłeś, że wiele starszych stacji roboczych z systemem Windows w sieci nie zostało odpowiednio załatanych i jest podatnych na ransomware WannaCry. Gdzie powinieneś zawrzeć te informacje w swoim raporcie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

22. Generujesz pisemny raport ustaleń po teście penetracyjnym. Podczas testu odkryłeś, że wiele starszych stacji roboczych z systemem Windows w sieci nie zostało odpowiednio załatanych i jest podatnych na ransomware WannaCry. Aby rozwiązać ten problem, klient musi zainstalować aktualizację MS17-010 — krytyczną aktualizację firmy Microsoft. Gdzie należy zawrzeć tę rekomendację w twoim raporcie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

23. Generujesz pisemny raport ustaleń po teście penetracyjnym. Porównujesz każdą lukę znalezioną w teście z bazą danych Common Vulnerabilities and Exposures (CVE), aby przypisać jej jakościową ocenę ryzyka: Niskie, Średnie, Wysokie lub Krytyczne. Gdzie te oceny ryzyka powinny znaleźć się w raporcie?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

24. Generujesz pisemny raport ustaleń po teście penetracyjnym. Na podstawie wyników testu stworzyłeś listę rekomendacji, na których Twoim zdaniem klient powinien się skupić. Gdzie w raporcie umieścić swoje rekomendacje?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

25. Generujesz pisemny raport ustaleń po teście penetracyjnym. W której części raportu należy wziąć pod uwagę apetyt na ryzyko klienta przy podejmowaniu decyzji, które informacje uwzględnić?

A. Streszczenie wykonawcze

B. Metodologia

C. Ustalenia i środki zaradcze

D. Metryki i miary

E. Wniosek

26. Organizacja niedawno dowiedziała się, że jej obiekt został zbudowany w odległości kilkuset jardów od linii uskoku. Kierownictwo podejmuje decyzję o wykupieniu rozszerzonej polisy ubezpieczeniowej, która pokryje utratę działalności w przypadku trzęsienia ziemi. . Jaki rodzaj reakcji na ryzyko opisano w tym scenariuszu?

A. Unikanie

B. Przeniesienie

C. Łagodzenie

D. Akceptacja

27. Podczas testu penetracyjnego Twoi testerzy odkryli, że mogą łatwo skopiować poufne dane na swoje osobiste urządzenia mobilne, a następnie wysłać te dane do odbiorców spoza organizacji, korzystając z mobilnego połączenia szerokopasmowego swoich urządzeń. Zalecasz wdrożenie systemu zarządzania urządzeniami mobilnymi (MDM). Klient uznał jednak, że taki środek jest zbyt kosztowny i skomplikowany do wdrożenia. W rzeczywistości nie wdrożą żadnego rodzaju kontroli, aby zapobiec takim sytuacjom w przyszłości. Jaki rodzaj reakcji na ryzyko opisano w tym scenariuszu?

A. Unikanie

B. Przeniesienie

C. Łagodzenie

D. Akceptacja

28. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Co powinieneś zrobić najpierw w procesie ustalania zakresu?

A. Negocjuj opłatę za test penetracyjny.

B. Przejrzyj wymagania PCI-DSS.

C. Ustaw harmonogram testu penetracyjnego.

D. Postaw się jako klient i odwiedź kilka witryn sklepowych, aby wstępnie ocenić organizację.

29. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Które z poniższych testów należy uwzględnić w ocenie? (Wybierz dwa.)

A. Fizyczny dostęp do danych posiadacza karty jest ograniczony.

B. Środowisko danych posiadacza karty (CDE) jest odizolowane od reszty sieci.

C. W przypadku zakupów kartą kredytową obowiązuje polityka zwrotów.

D. Obowiązuje polityka obciążeń zwrotnych.

E. Kasjerzy są zobowiązani do sprawdzenia podpisu na karcie za pomocą podpisu klienta.

30. Właśnie spotkałeś się z nowym klientem, który poprosił Cię o wykonanie dla niego testu penetracyjnego. Klient zarządza szeregiem sklepów detalicznych, które akceptują karty kredytowe. Musisz ocenić, czy są zgodne z PCI-DSS. Które z poniższych testów należy uwzględnić w ocenie? (Wybierz dwa.)

A. Używaj wyłącznie sprzętu certyfikowanego przez Microsoft jako zgodnego z systemem Windows 100.

B. Szyfruj transmisję danych posiadacza karty.

C. Upewnij się, że tylko jedno konto użytkownika jest używane przez wszystkich pracowników w celu uzyskania dostępu do zasobów sieciowych i danych posiadaczy kart.

D. Użyj routera NAT, aby odizolować środowisko danych posiadacza karty (CDE) od reszty sieci.

E. Usuń wszystkie domyślne hasła z oprogramowania i urządzeń sprzętowych.

31. Który typ skanowania podatności jest najmniej inwazyjny w sieci docelowej?

A. Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

32. Jaki typ skanowania w poszukiwaniu luk najprawdopodobniej zostanie wykryty przez system zapobiegania włamaniom (IPS) lub system wykrywania włamań (IDS)?

Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

33. Jaki typ skanowania podatności jest najmniej prawdopodobnie wykryty przez system zapobiegania włamaniom (IPS) lub system wykrywania włamań (IDS)?

Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

34. Który typ skanowania podatności będzie częściej używany przez obrońcę niż przez testera penetracyjnego?

Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

35. Jaki typ skanowania podatności wysyła pakiety SYN do hostów sieciowych w celu ich wyliczenia?

Odkrycie

B. Pełny

C. Ukrycie

D. Zgodność

36. Jaki rodzaj exploita nakłania serwer sieciowy do prezentowania przeglądarce internetowej użytkownika połączenia HTTP zamiast połączenia HTTPS, jak pierwotnie żądał użytkownik?

A. SSL stripping

B. Relay attack

C. NAC bypass

D. Cross-site scripting

37. Jaki jest najlepszy sposób obrony przed atakiem SSL stripping?

A. Zaktualizuj definicje wirusów na stacjach roboczych użytkowników.

B. Zaimplementuj urządzenie do wykrywania włamań do sieci (NID).

C. Zaimplementuj ścisłe zasady HSTS, które uniemożliwiają przeglądarce użytkownika otwieranie strony, chyba że zostało użyte połączenie HTTPS.

D. Ponownie skonfiguruj wszystkie przeglądarki, aby wymagały sesji TLS.

38. Podczas testu penetracyjnego szarej skrzynki tester działa jako człowiek pośrodku między serwerem WWW a stacją roboczą użytkownika końcowego. Gdy przeglądarka użytkownika żąda strony z serwera WWW przy użyciu protokołu TLS 1.2, tester zmienia żądanie i określa, że zamiast tego do ochrony sesji należy użyć protokołu SSL 2.0. Jaki rodzaj exploita wystąpił w tym scenariuszu?

A. SSL stripping

B. Downgrade

C. NAC bypass

D. Replay attack

39. Podczas testu penetracyjnego szarej skrzynki tester chce wdrożyć atak typu downgrade man-inthe-middle, aby zmniejszyć bezpieczeństwo sesji przeglądarki internetowej z TLS na SSL. Jakiego exploita może użyć atakujący, aby nakłonić klienckie stacje robocze do myślenia, że jej stacja robocza jest serwerem sieciowym i odwrotnie?

A. ARP spoofing

B. Replay attack

C. Pass the Hash

D. SYN attack

40. Podczas testu penetracyjnego szarej skrzynki tester decyduje się przeprowadzić test warunków skrajnych serwera plików organizacji docelowej, wysyłając mu powódź półotwartych połączeń TCP, które w rzeczywistości nigdy nie są ukończone. Co to za exploit?

A. Denial of service (DoS)

B. Distributed denial of service (DDoS)

C. Replay attack

D. NAC bypass

41. Które narzędzie zdalnego dostępu zostało stworzone przez organizację, która opracowała nmap jako zaktualizowaną wersję narzędzia netcat obsługującego szyfrowane tunele danych?

A. Framework Metasploit

B. SET

C. hping

D. ncat

42. Podczas testu penetracyjnego szarej skrzynki tester chce mieć możliwość skonfigurowania exploita powłoki wiązania, w którym na skompromitowanym systemie docelowym zostanie skonfigurowany słuchacz. Jakich narzędzi dostępu zdalnego można do tego użyć?

A. ncat

B. netcat

C. Powersplot

D. DAST

E. SAST

43. Które narzędzie mobilne zapewnia strukturę ataku, którą można wykorzystać do wykorzystania urządzeń mobilnych z systemem operacyjnym Android?

A. APKX

B. Studio APK

C. Drozer

D. DAST

44. Jakiego narzędzia mobilnego można użyć do inżynierii wstecznej pliku APK z urządzenia mobilnego z systemem operacyjnym Android?

A. Peach

B. APK Studio

C. Drozer

D. DAST

45. Które narzędzie mobilne to wrapper Pythona, który może wyodrębnić kod źródłowy Java bezpośrednio z pliku wykonywalnego APK Androida?

A. APKX

B. AFL

C. Drozer

D. DAST

46. Które z poniższych jest przykładem uwierzytelniania dwuskładnikowego (2FA)?

A. Nazwa użytkownika + hasło

B. Nazwa użytkownika + PIN

C. Nazwa użytkownika + PIN + skan rozpoznawania twarzy

D. PIN + skanowanie linii papilarnych + token bezpieczeństwa

47. Które z poniższych jest przykładem uwierzytelniania trójskładnikowego (3FA)?

A. Nazwa użytkownika + hasło + token bezpieczeństwa

B. Nazwa użytkownika + PIN + skan linii papilarnych + hasło jednorazowe (OTP)

C. Nazwa użytkownika + PIN + skan rozpoznawania twarzy

D. Hasło + PIN + token bezpieczeństwa

48. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach informujesz, że aplikacja internetowa opracowana we własnym zakresie i używana przez organizację do zarządzania zamówieniami klientów jest podatna na ataki typu SQL injection. Co powinieneś polecić klientowi, aby temu zaradzić?

A. Przepisz kod, aby oczyścić dane wejściowe użytkownika.

B. Zaszyfruj wszystkie dane przed przesłaniem ich w sieci.

C. Zaszyfruj wszystkie dane w spoczynku w bazie danych.

D. Zastąp aplikację aplikacją komercyjną, która pełni podobną funkcję.

49. Właśnie zakończyłeś test penetracyjny dla klienta. W swoich ustaleniach informujesz, że aplikacja internetowa opracowana we własnym zakresie i używana przez organizację do zarządzania zamówieniami klientów jest podatna na ataki typu SQL injection. Co powinieneś polecić klientowi, aby temu zaradzić?

A. Dane ucieczki.

B. Implementuj SSL dla komunikacji sieciowej.

C. Wymagaj 2FA podczas uwierzytelniania użytkowników.

D. Posolić hasz.

50. Jaka obrona przed atakami typu SQL injection polega na użyciu przygotowanych instrukcji SQL ze zmiennymi ograniczonymi?

A. Odkażanie danych wprowadzonych przez użytkownika

B. Ucieczka danych

C. Parametryzacja zapytań

D. Kluczowe rozciąganie

51. Przeprowadzasz test penetracyjny białej skrzynki. Zakres testu określa, że test zostanie przeprowadzony na przełącznikach, routerach i firewallach organizacji. Ponieważ ocena zbliża się do końca, klient prosi o wykorzystanie pozostałego czasu również na przetestowanie jej serwerów pocztowych. Co wydarzyło się w tym scenariuszu?

A. Obracanie

B. Testowanie oparte na celach

C. Pełzanie zakresu

D. Testowanie oparte na celach

52. Przeprowadzasz test penetracyjny organizacji, która przetwarza karty kredytowe. Klient poprosił, aby zakres testu był oparty na standardzie PCI-DSS. Jaki rodzaj oceny występuje w tym scenariuszu?

A. Ocena oparta na zgodności

B. Ocena oparta na celach

C. Ocena drużyny czerwonej

D. Ocena oparta na celach

53. Negocjujesz nadchodzący test penetracyjny z nowym klientem. W umowie uwzględniłeś język, który określa, że wyniki testu są ważne tylko w momencie wykonania testu. Dlaczego ten język jest w umowie?

A. Test penetracyjny może wyłączyć krytyczne systemy.

B. Naprawa sieci po zakończeniu testu może zająć trochę czasu.

C. Przyszłe zmiany technologiczne mogą ujawnić nowe luki w zabezpieczeniach, które są obecnie nieznane.

D. Test penetracyjny będzie wykorzystywał te same narzędzia i techniki, które są dostępne dla prawdziwych napastników.

54. Negocjujesz nadchodzący test penetracyjny z nowym klientem. W umowie uwzględniłeś język, który określa, że zakres i metodologia wymagana przez klienta mogą wpłynąć na kompleksowość testu. Dlaczego ten język jest w umowie?

A. Po zakończeniu testu naprawa sieci może zająć trochę czasu.

B. Zasady zaangażowania i rodzaj stosowanej oceny mogą uniemożliwić wykrycie pewnych podatności.

C. Test penetracyjny będzie wykorzystywał te same narzędzia i techniki, które są dostępne dla prawdziwych napastników.

D. Zasady zaangażowania i rodzaj stosowanej oceny powinny zapewnić, że wszystkie znane luki zostaną zidentyfikowane.

55. Negocjujesz nadchodzący test penetracyjny z nowym klientem. Poprosili o wykonanie testu „wiedzy zerowej" ich sieci. Jaki rodzaj testu penetracyjnego należy wykonać?

A. Czarna skrzynka

B. Szare pudełko

C. Białe pudełko

D. Oparte na zgodności

56. Oceniasz wyniki skanowania podatności i zauważasz, że wiele urządzeń sieciowych, takich jak routery i punkty dostępowe, nadal używa domyślnych administracyjnych nazw użytkowników i haseł. Informacje te można łatwo znaleźć w Internecie i stanowią istotną lukę w zabezpieczeniach. Co powinieneś zrobić? (Wybierz dwa.)

A. Zalecamy, aby klient przyjął najlepszą praktykę zmiany wszystkich domyślnych nazw użytkowników i haseł.

B. Wykorzystaj urządzenia, które używają domyślnych nazw użytkowników i haseł.

C. Ręcznie zmień domyślne nazwy użytkownika i hasła klienta.

D. Opublikuj fakt, że klient nadal używa domyślnych nazw użytkownika i haseł na popularnym internetowym forum cyberbezpieczeństwa.

57. Właśnie zakończyłeś skanowanie sieci docelowej i teraz

nadanie priorytetu działaniom przygotowującym do wykorzystania wykrytych luk w zabezpieczeniach. Odkrywasz, że organizacja nadal korzysta z kilku starszych systemów Windows Server 2003, które nie zostały odpowiednio zaktualizowane i są podatne na określony exploit. Postanawiasz napisać mały program, który wykorzysta ten exploit. Jednak używasz Kali Linux prawie wyłącznie. Co należy zrobić, aby napisać program Windows? (Wybierz dwa.)

A. Napisz kod w C w swoim systemie Linux.

B. Wykorzystaj łańcuch exploitów.

C. Napisz kod w C++ na laptopie z systemem Windows.

D. Krzyżowo skompiluj kod.

E. Implementuj brutalne wymuszanie poświadczeń.

58. Właśnie zakończyłeś skanowanie sieci docelowej i teraz nadajesz priorytet działaniom przygotowującym do wykorzystania znalezionych luk. Odkrywasz, że organizacja nadal używa kilku starszych nieobsługiwanych systemów Windows 2000 Server. Po przeprowadzeniu pewnych badań identyfikujesz kilka luk w zabezpieczeniach związanych z tymi systemami, które można wykorzystać. Modyfikujesz kod źródłowy konkretnego exploita tak, aby działał na tych starszych systemach, a następnie go kompilujesz. Jak nazywają się procesy użyte w tym scenariuszu? (Wybierz dwa.)

A. Cross-kompilacja kodu

B. Modyfikacja exploitów

C. Łączenie exploitów

D. Mapowanie podatności na potencjalne exploity

E. Opracowanie dowodu koncepcji

59. Właśnie zakończyłeś skanowanie sieci docelowej i jesteś teraz

nadanie priorytetu działaniom przygotowującym do wykorzystania wykrytych luk w zabezpieczeniach. System, który chcesz zaatakować, nie może zostać naruszony za pomocą jednego exploita. Jednak ustalasz, że możesz użyć wielu exploitów w połączeniu ze sobą, aby złamać system. Pierwszy z nich przechodzi przez zaporę systemową opartą na hoście. Drugi wykorzystuje konto użytkownika ze słabym hasłem. Trzeci podnosi uprawnienia w systemie. Jak nazywa się twoje rozwiązanie?

A. Oszustwo

B. Modyfikacja exploitów

C. Łączenie exploitów

D. brutalne forsowanie poświadczeń

E. Opracowanie dowodu koncepcji

60. Właśnie zakończyłeś skanowanie sieci docelowej i teraz nadajesz priorytet działaniom przygotowującym do wykorzystania znalezionych luk. Odkrywasz, że organizacja nadal używa kilku starszych nieobsługiwanych systemów Windows 2000 Server. Po przeprowadzeniu pewnych badań identyfikujesz kilka luk w zabezpieczeniach związanych z tymi systemami, które można wykorzystać. Modyfikujesz kod źródłowy konkretnego exploita tak, aby działał na tych starszych systemach, a następnie go kompilujesz. Co powinieneś zrobić dalej?

A. Atakuj systemy docelowe.

B. Przetestuj zmodyfikowany exploit na maszynach wirtualnych w środowisku laboratoryjnym.

C. Implementuj brutalne forsowanie poświadczeń.

D. Krzyżowo skompiluj kod.

61. Która z poniższych usług jest usługą działającą w systemie Windows i wymuszającą politykę bezpieczeństwa systemu?

A. LSASS

B. Centrum dystrybucji kluczy (KDC)

C. Obiekt zasad grupy (GPO)

D. LDAP

62. Która funkcja systemu Windows może potencjalnie umożliwić przesyłanie poświadczeń uwierzytelniania jako zwykłego tekstu przez połączenie sieciowe?

A. Instalacje nienadzorowane przez PXE

B. debugowanie JTAGTAG

C. Pulpit zdalny

D. Dołączenie do domeny

63. Co jest przechowywane w bazie danych SAM w systemie Windows?

A. Wpisy dziennika bezpieczeństwa Security

B. Podpisy cyfrowe powiązane z każdą aplikacją zainstalowaną w systemie

C. Ustawienia zasad grupy

D. Zaszyfrowane hasła do kont

64. Podczas testu penetracyjnego szarej skrzynki tester tworzy kampanię phishingową, która nakłania użytkowników do pobrania aplikacji konia trojańskiego, która po cichu zastępuje plik biblioteki dołączanej dynamicznie w systemie lokalnym zmodyfikowaną wersją, która po uruchomieniu ładuje keylogger. Jak nazywa się ten rodzaj exploita?

A. JTAG debug

B. Cold boot attack

C. cPassword

D. DLL hijacking

65. Które z poniższych są sposobami wykorzystania usług w systemie Windows? (Wybierz dwa.)

A. Korzystanie z nienotowanych ścieżek usług

B. Zastępowanie plików wykonywalnych usługami do zapisu

C. Wdrożenie ataku zimnego rozruchu

D. Naruszanie poświadczeń w LSASS

66. Musisz stworzyć skrypt Rubiego, który poprosi użytkownika o wprowadzenie wartości. Które polecenie zaakceptuje wartość wprowadzoną przez użytkownika i przypisze ją do zmiennej o nazwie TargetHost?

A. TargetHost = input('Please enter a hostname:')

B. read TargetHost

C. TargetHost = gets

D. $TargetHost = read-host -Prompt

67. Która komenda w skrypcie Rubiego spowoduje zapisanie na ekranie wartości zmiennej o nazwie TargetHost?

A. echo $TargetHost

B. print (TargetHost)

C. writeln TargetHost

D. puts TargetHost

68. Musisz stworzyć skrypt Pythona, który poprosi użytkownika o wprowadzenie wartości. Które polecenie zaakceptuje wartość wprowadzoną przez użytkownika i przypisze ją do zmiennej o nazwie TargetHost?

A. TargetHost = input('Please enter a hostname:')

B. read TargetHost

C. TargetHost = gets

D. $TargetHost = read-host -Prompt

69. Które polecenie w skrypcie Pythona spowoduje zapisanie na ekranie wartości zmiennej o nazwie TargetHost?

A. echo $TargetHost

B. print (TargetHost)

C. writeln TargetHost

D. puts TargetHost

70. Który z poniższych elementów musi znajdować się na początku każdego skryptu Basha?

A. #Comment

B. #!/bin/bash

C. exit 0

D. #begin script

71. Jesteś testerem penetracji i zostałeś poproszony przez klienta o przetestowanie bezpieczeństwa kilku serwerów internetowych. Możesz uzyskać dostęp do roota/administratora na kilku serwerach, wykorzystując luki związane z korzystaniem z DNS, FTP, IMAP, POP, SMTP i Telnet. Co powinieneś polecić swojemu klientowi, aby lepiej chronić jego serwery internetowe?

O. Powinni wyłączyć wszelkie niepotrzebne usługi.

B. Powinny zwiększyć rejestrowanie zdarzeń aplikacji.

C. Powinni używać honeypota.

D. Powinni używać Transport Layer Security (TLS).

72. Przeprowadziłeś test penetracyjny i przeglądasz wyniki. Zauważasz, że organizacja używa tego samego hasła administratora lokalnego we wszystkich systemach. Jakiego narzędzia możesz użyć, aby rozwiązać ten problem?

A. Rozwiązanie hasła administratora lokalnego (LAPS)

B. Ograniczona pomoc administratora hasła (LAPA)

C. Nessusa

D. Metasplot

73. Jesteś analitykiem bezpieczeństwa i właśnie ukończyłeś test penetracyjny. Która pozycja nie byłaby odpowiednia podczas pisania streszczenia?

A. Opis wszystkich Twoich ustaleń i słabych punktów.

B. Oświadczenie o ryzyku dla wszystkich znalezionych podatności.

C. Powinien być napisany prostym językiem.

D. Uwzględnij wszystkie szczegóły techniczne dotyczące testowania.

74. Jesteś testerem penetracyjnym i przeprowadzasz porządki po zaangażowaniu. Jakie czynności są wykonywane podczas fazy porządkowania po zaangażowaniu? (Wybierz trzy.)

A. Naprawa wszystkich luk w zabezpieczeniach

B. Usunięcie wszelkich użytych narzędzi

C. Usuwanie muszli

D. Usunięcie danych uwierzytelniających stworzonych przez testera

75. Ty i kolega omawiacie scenariusz organizacji wdrażającej filtrowanie treści wiadomości e-mail w celu blokowania wiadomości przychodzących, które wydają się pochodzić ze źródeł wewnętrznych bez odpowiedniego uwierzytelnienia. Organizacja może również odfiltrować wszelkie wiadomości zawierające słowa kluczowe wysokiego ryzyka lub wyglądające na pochodzące ze znanych złośliwych źródeł. Do jakiej wspólnej kategorii działań remediacyjnych należałoby to?

A. Pomiar

B. Ludzie

C. Proces

D. Technologia

76. DirBuster to wielowątkowa aplikacja Java, która może wymusić brute-force nazwy plików i katalogi na serwerach WWW i aplikacjach internetowych przy użyciu jakiego typu słownika?

A. Lista

B. Lista słów

C. Lista aplikacji

D. Webster

77. Co nazywa się standardem IEEE używanym do rozwiązania problemu debugowania i podłączania do urządzeń wbudowanych na płytce drukowanej?

A. JTAG

B. RMF

C. Xcode

D. Clutch

78. SSH i iProxy to dwa sposoby łączenia się z iDevice po jailbreaku. Jeśli iDevice ulegnie awarii i będziesz musiał ponownie nawiązać łączność, jaki jest najłatwiejszy sposób na zapewnienie, że na laptopie z systemem MacOS nie będą nadal uruchomione żadne procesy iProxy?

A. iproxy stop

B. killall iproxy

C. kill iproxy

D. kill -9 <process id>

79. Po zainstalowaniu aplikacji mobilnej klienta ze Sklepu Google Play na iPhone'a z jailbreakiem, następnym krokiem jest zrzucenie pakietu aplikacji do IPA za pomocą Clutch, aby można było go użyć do przeprowadzenia analizy statycznej. Gdzie domyślnie Clutch przechowuje postprocessing plików IPA?

A. /var/tmp/clutch

B. /var/tmp

C. /tmp

D. /storage

80. Pliki listy właściwości (plist) zawierają dane konfiguracyjne dotyczące aplikacji zainstalowanej na iOS. Domyślnie najlepsze praktyki firmy Apple w zakresie bezpieczeństwa implementują funkcję zabezpieczeń o nazwie App Transport Security (ATS), aby poprawić prywatność i integralność danych. Istnieje jednak sposób na obejście tego w ustawieniach aplikacji w pliku plist. Jak nazywa się klucz używany do kontrolowania zachowania połączeń HTTP?

A. NSAppleScriptEnabled

B. NSAppTransportSecurity

C. NSAllowsLocalNetworking

D. NETestAppMapping