МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Кафедра комп’ютерних наук та кібербезпеки

Глинчук Л. Я.

ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: МЕТОДИЧНІ ВКАЗІВКИ ДЛЯ ПІДГОТОВКИ ДО ПІДСУМКОВОГО КОНТРОЛЮ

для студентів спеціальності 125 Кібербезпека
першого (бакалаврського) рівня

Луцьк 2023

УДК 004.4(072)
Г 54

Рекомендовано до видання науково-методичною радою Волинського національного університету імені Лесі Українки (протокол № 7 від 13 березня 2023 р.)

Рецензенти:

Волошина Т.В. – кандидат фізико-математичних наук, доцент кафедри математичного аналізу та статистики Волинського національного університету імені Лесі Українки;

Багнюк Н.В. – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Луцького національного технічного університету.

Діагностика шкідливого програмного забезпечення: методичні вказівки для підготовки до підсумкового контролю. [Електронний ресурс] / укладач Л. Я. Глинчук; ВНУ ім. Лесі Українки. Електронні текстові данні (1 файл: 232 КБ). Луцьк : ВНУ ім. Лесі Українки, 2023. 74 с.

Методичні вказівки призначені для студентів спеціальності 125 Кібербезпека першого (бакалаврського) рівня. Містять тестові питання для повторення теоретичного матеріалу з предмету «Діагностика шкідливого програмного забезпечення» та перелік практичних завдань для підготовки до підсумкового контролю. Теоретичні питання були підготовлені згідно тем силабусу предмету та відповідають теорії, що розглядається на відповідних лекційних заняттях. Практичні завдання укладенні згідно лабораторних робіт, але дещо спрощені та розділені.

Тестові питання для повторення теоретичного матеріалу

1. Шкідливе програмне забезпечення – це ... (виберіть 2 пункти)

   - програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем

   - скрипт, який служить для аналізу поведінки певного ПЗ на комп’ютері

   - це різні форми шкідливого коду незалежно від способу його поширення та поведінки, а також заподіяної ним шкоди

   - програмне забезпечення, яке встановлює на ПК користувач

2. Таку дію: внесення змін у файли, зміна структури розміщення файлів на диску. Виконує ...

   - дефективне ПЗ

   - шпигунське ПЗ

   - шкідливе ПЗ

   - рекламне ПЗ

3. Такі дії: виведення звукових або текстових повідомлень, спотворення зображення на екрані монітора; примусове перезавантаження операційної системи. Виконує ...

   - операційна система

   - шкідливе ПЗ

   - спеціальні утиліти

4. Політика безпеки, яку дійсно можна назвати хорошою і ефективною, повинна

   - бути зрозуміла адміністраторам системи

- бути зрозуміла всім користувачам
- бути зрозуміла керівникам
- бути зрозуміла ІТ професіоналам

5. Діагностичні програми дозволяють перевірити роботу ...
   - ПЗ, що встановлено на ПК
   - як всієї системи, так і окремих її вузлів
   - окремих її вузлів
   - апаратної складової

6. Визначення несправності ПК складається з наступних етапів ...
   - первинна діагностика
   - мережна діагностика
   - програмна діагностика
   - апаратна діагностика
   - повна діагностика
   - вторинна діагностика

7. Діагностика комп'ютера на програмному рівні знадобиться, якщо: (виберіть декілька пунктів)
   - техніка не вмикається
   - на екрані з’являються незрозумілі картинки
   - самостійно вимикається
   - комп'ютер зависає

- з’являються незрозумілі звуки
- перезавантажується без причини
- повільно працює

8. У складі ОС є декілька діагностичних програм?
   - так
   - ні, немає, потрібно встановлювати

9. Згідно схеми іменування шкідливих програм Microsoft, платформа шкідливого ПЗ Worm:Win32/Allaple.A ...
   - Worm
   - Win32
   - Allaple
   - A

10. Що означає "платформа" для шкідливого ПЗ?
    - структурної подібності між різними шкідливими програмами
    - операційну систему, на якій шкідливе ПЗ призначене працювати
    - основну діяльність, яку виконує зловмисне програмне забезпечення

11. За рівнем небезпечності дій шкідливі програми розподіляють на ...
    - небезпечні, віруси, соціальна інженерія
    - безпечні, небезпечні, дуже небезпечні
    - безпечні, хробаки, трояни

12. Шкідливе ПЗ за наявністю матеріальної вигоди ...

- хуліганство, жарт
- крадіжка, шифрування файлів
- ізоляція операційної системи
- самоствердження
- отримання контролю над віддаленими комп'ютерними системами

13. Доцільно також класифікувати шкідливе програмне забезпечення за двома головними ознаками ...

- крадіжка, шифрування файлів
- за наявністю матеріальної вигоди
- за метою розробки
- способом розповсюдження засобу, метою функціонування засобу

14. Шкідливе програмне забезпечення поділяють на дві категорії

- таке, що виконує деструктивні функції, і таке, що їх не виконує
- таке, що виконує функції програмних закладок і не виконує
- таке, що має доступ до мережі і не має

15. Де можна подивитися орієнтовну вірусну енциклопедію, яку використовує певний антивірусний продукт?

- на офіційному сайті розробника ПЗ

- на форумі користувачів
- на ресурсі ІТ-спеціалістів ХАБР

16. Найбільш популярні джерела зараження ПК:

- апаратні та програмні закладки
- соціальна мережа, сарафанне радіо, відеоролики
- Інтернет, електронна пошта, зовнішні накопичувачі

17. Лікуванню підлягають лише файли заражені ..., інші типи шкідливого ПЗ потрібно просто видаляти

- руткітами
- бекдорами
- рекламними модулями
- вірусами

18. Яку тенденцію ви помітили у випадку створення нового шкідливого ПЗ? З роками його кількість зменшується чи збільшується? (Згідно переглянутого графіка на лекціях)

- то збільшується, то зменшується
- тільки збільшується
- як не дивно, але зменшується

19. Шкідливе ПЗ, яке знищує дані з постійної та зовнішньої пам’яті, виконує шпигунські дії тощо, називається ...

- безпечним
- дуже небезпечним

- небезпечним

20. Комп'ютерна програма, яка має здатність до прихованого самопоширення – це

- шпигунське ПЗ
- рекламні модулі
- соціальна інженерія
- комп’ютерний вірус

21. Комп'ютерні віруси бувають декількох типів, а саме ... (виберіть декілька пунктів)

- Шкідник
- Знищувач
- Експлойти
- Хробак
- Руткіти
- Жарт
- Трояни
- Комбінований

22. Хто, коли і навіщо створював перші комп’ютерні віруси?

- Військові, у 70-х роках для атак під час "Холодної війні"
- Підлітки у 80-х роках ХХ ст. заради цікавості

- Джон фон Нейман на практичних заняттях в Нью-Йоркському університеті у 40-х роках XX ст.

- Вчені хіміки у 55-х роках XX ст. для наукового прориву

23. Яке джерело зараження ПК було основним на початку 2000-х років?

- Атаки через браузери

- Зовнішні накопичувачі

- Електронна пошта

- RSS-канал

24. Які найпопулярніші типи загроз в Україні?

- Криптувальники

- Файлові віруси

- Рекламні модулі

- Банківські троянці

25. Тип вірусу який не завдає шкоди, а просто лякає ...

- Знищувач

- Експлойт

- Хробак

- Руткіти

- Жарт

- Трояни

- Комбінований

26. Віруси за середовищем їх існування поділяються на …

- нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси

- резидентні віруси, нерезидентні віруси

- перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси

- файлові віруси, мережні віруси, завантажувальні віруси, макро-віруси

27. За активністю віруси прийнято поділяти на ...

- нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси

- резидентні віруси, нерезидентні віруси

- перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси

- файлові віруси, мережні віруси, завантажувальні віруси, макро-віруси

28. За деструктивними можливостями віруси можна поділити на ...

- нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси

- резидентні віруси, нерезидентні віруси

- перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси

- файлові віруси, мережні віруси, завантажувальні віруси, макро-віруси

29. Класифікаційний код вірусу ...

- формалізований список основних властивостей
- складається з літерного префікса, кількісної характеристики і факультативного літерного суфікса
- рядок для контекстного пошуку даного вірусу в зараженій програмі

30. Дескриптор вірусу ...

- формалізований список основних властивостей
- складається з літерного префікса, кількісної характеристики і факультативного літерного суфікса
- рядок для контекстного пошуку даного вірусу в зараженій програмі

31. Сигнатура вірусу ...

- формалізований список основних властивостей
- складається з літерного префікса, кількісної характеристики і факультативного літерного суфікса
- рядок для контекстного пошуку даного вірусу в зараженій програмі

32. Основне завдання комп'ютерного троянського коня:

- використати обчислювальні ресурси пристроїв для видобування криптовалют
- сканувати різні типи вразливостей програмного забезпечення

- проникнути в систему під виглядом якоїсь корисної, або хоча б невинної, програми

33. Як по іншому можна назвати стелс-вірус?

- бекдор
- вірус-невидимка
- руткіт
- троян

34. Залежно від типу дії, троянів можна розділити на наступні види: (виберіть декілька пунктів)

- Віддалений доступ (Backdoors)
- Експлойти
- Дезактиватори (FakeAV)
- DoS-атаки
- Стелс-троян

35. Стелс-технології призначені для ...

- розробки макро-вірусів
- зменшення помітності об'єкта
- перехоплення повідомлень

36. Макро-віруси …

- впроваджуються в основному у виконувані файли, тобто у файли з розширеннями COM та EXE

- заражають файли-документи і електронні таблиці відомих програмних продуктів

- використовують для свого розповсюдження протоколи або команди комп'ютерних мереж та електронної пошти

37. Мережні віруси …

- впроваджуються в основному у виконувані файли, тобто у файли з розширеннями COM та EXE

- заражають файли-документи і електронні таблиці відомих програмних продуктів

- використовують для свого розповсюдження протоколи або команди комп'ютерних мереж та електронної пошти

38. Якщо вплив вірусу обмежується зменшенням вільної пам'яті на диску і графічними, звуковими та іншими ефектами, то цей вірус можна назвати:

- нешкідливим вірусом

- безпечним вірусом

- небезпечним вірусом

39. Якщо вірус ніяким чином не впливає на роботу комп'ютера, крім зменшення вільної пам'яті на диску в результаті свого поширення, то такий вірус можна назвати:

- нешкідливим вірусом

- безпечним вірусом

- небезпечним вірусом

40. Троянська програма може виконувати такі дії: (виберіть 4 пункти)

- крадіжка облікових записів (логіну і пароля) для доступу до популярних ресурсів і програм
- головним завданням є дзвінки на платні телефонні лінії з метою отримання грошей від користувача шляхом виставлення рахунків за телефонні дзвінки
- розмноження за допомогою програм для спілкування, таких як ICQ, Skype, MSN Messenger і т.п.
- крадіжка адрес електронної пошти збережених на комп'ютері
- ведення шпигунства за користувачем
- здатна викликати некоректну роботу програмного забезпечення, і тим самим надати зловмисникові (шкідливій програмі) контроль над системою або ж порушити її функціонування
- знищення всієї інформації на комп’ютері без можливості її відновлення

41. Загрози для дітей в мережі Інтернет: (виберіть декілька пунктів)

- кіберагресія
- віртуальний терор, найчастіше підлітковий
- соціальна мережа Facebook
- хмарні технології
- кібербулінг, тролінг, флеймінг
- обліковий запис
- доступ до шкідливого й нелегального контенту (популяризація порнографії, віртуальних наркотиків, суїциду тощо).

42. Хепіслепінг ...

- це обмін власними фото/ відео/текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж

- це улюблений метод «тролів» (провокаторів), що полягає в обміні короткими, гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях Інтернету: на чатах, форумах, у дискусійних групах, спільнотах. Інколи він перетворюється у затяжну війну.

- один із видів кібербулінгу, його назва походить від випадку в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефону. Тепер ця назва закріпилася за будь- якими відеороликами з записами реальних сцен насильства.

43. Флеймінг ...

- це обмін власними фото/ відео/текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж

- це улюблений метод «тролів» (провокаторів), що полягає в обміні короткими, гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях Інтернету: на чатах, форумах, у дискусійних групах, спільнотах. Інколи він перетворюється у затяжну війну.

- один із видів кібербулінгу, його назва походить від випадку в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефону. Тепер ця назва закріпилася за будь-якими відеороликами з записами реальних сцен насильства.

44. Секстинг ...

- це обмін власними фото/ відео/текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж

- це улюблений метод «тролів» (провокаторів), що полягає в обміні короткими, гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях Інтернету: на чатах, форумах, у дискусійних групах, спільнотах. Інколи він перетворюється у затяжну війну.

- один із видів кібербулінгу, його назва походить від випадку в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефону. Тепер ця назва закріпилася за будь- якими відеороликами з записами реальних сцен насильства.

45. Інтернет-залежність це ...

- це важлива емоція, яка попереджує нас про небезпеку і мобілізує до відповідних дій. У нашому мозку функціонує комплексна система тривоги. Вона дає нам змогу вчасно помічати загрози та запобігати їм.

- психічний розлад, нав'язливе бажання вийти в Інтернет і хвороблива нездатність вчасно відключитися від нього. Це явище може спричинити стан, у якому людина фокусуватиметься на віртуальному, а не реальному світі.

- проявляється у побитті інших людей, у вербальних образах, погрозах, ворожих насмішках, жартах

46. Як діти мають вчитись використовувати Інтернет?

- Навчатись у друзів та однолітків

- Навчатися за допомогою батьків

- Не мають навчатися – це вроджена навичка нового покоління

47. Що насамперед потрібно зробити, якщо дитина переглядає шкідливий контент?

- Забрати в неї телефон (планшет)
- Спільно з дитиною придумати покарання
- Визначити, чи навмисно вона шукала такі матеріали

48. Чому підлітки надсилають свої інтимні фото «друзям» в соціальних мережах? Оберіть усі правильні відповіді.

- Тому що це для них гра або спосіб виразити свою близькість до отримувача фото
- Внаслідок примусу або шантажу зі сторони отримувача фото
- Через психологічні проблеми, що переживає дитина

49. Чим кібербулінг відрізняється від звичайного булінгу?

- Діти легше переживають кібербулінг, адже він відбувається онлайн, а отже, він – несправжній
- Діти тяжко переживають і традиційний, і кібербулінг, адже обидва цькування негативно впливають на психічний стан та самооцінку дитини

50. Який контент не рекомендовано виставляти у соціальних мережах?

- Свою адресу
- Номер телефону
- Фотографії, на яких видно номер школи дитини

- Не рекомендовано виставляти, все, що описано вище

51. Соціальна інженерія (безпека) − це ...

- прихований майнінг
- злочинне вивідування даних
- моделювання та прогнозування стану ПК
- технологічний напрям соціології, що ґрунтується на критичному і дієвому ставленні до процесів соціальних змін у суспільстві

52. Виберіть з наведеного нижче, що відноситься до методів соціальної інженерії (виберіть 4 пункти)

- Фішинг
- Вішинг
- Соцінг
- Майнінг
- Складна атака через проміжну ціль («Supply chain attack»)
- Брифінг
- SMS-фішинг

53. Виберіть з наведеного нижче, що відноситься до методів соціальної інженерії (виберіть 3 пункти)

- «Кві про кво» (від лат. Quid pro quo)
- «Технічна соціальна інженерія»
- «Дорожнє яблуко» («road apple»)

- «Зворотна соціальна інженерія»
- Публікування своїх персональних даних

54. Виберіть психологічні прийоми, які використовуються в соціальній інженерії (виберіть 3 пункти)

- Взаємність
- Соціальний конформізм
- Контент
- Послідовність
- Електрична інженерія

55. Виберіть психологічні прийоми, які використовуються в соціальній інженерії (виберіть 3 пункти)

- Авторитет
- Електрична інженерія
- Симпатія
- Психологічна атака
- Дефіцит

56. Поняття соціальної інженерії було введено ...

- Кевіном Митником
- Дрорджем Блестоном
- Олександром Хорошко

57. Шкідливі програми для прихованого майнінгу належать до категорії ...

- соціальної інженерії та метою є спонукання людей робити певні дії, які вони за звичних умов ніколи не вчинили

- де зловмисники не чекають поки користувачі самі потраплять на підроблений сайт, а самі спонукають їх це зробити

- шкідливого коду, призначеного для використання обчислювальної потужності пристрою користувача з метою видобутку криптовалюти. При цьому, жертви не дають згоду і навіть не підозрюють про таку діяльність.

58. Криптомайнінг і криптоджекінг потребують ...

- рекламної презентації продукту компанії

- надзвичайно високої активності процесора

- розширений аналіз загроз

59. Як спробувати виявити прихований майнінг? (Запідозрити його роботу)

- перезавантажити операційну систему

- перейти в диспетчер задач і подивитися на скільки відсотків завантажений процесор

- скористатися спеціальними утилітами для пошуку

60. Чим відрізняється вірус від майнера?

- віруси шкодять системі, крадуть дані і т.д., майнери використовують технічні ресурси

- віруси шкодять роботі ПК, майнери блокують мережу

- віруси шпигують за користувачами, майнери крадуть персональні дані

61. Виявити сторонні файли, що запускають прихований майнінг, можуть ...

- спеціальні системи захисту
- звичайні антивірусні програми і утиліти для сканування ПК
- програми для моніторингу мережі

62. Чи загрози для мобільних телефонів інші чи такі ж як і для ПК?

- Ні, бо мобільний телефон має свою особливу ОС
- Так

63. Як називаються шпигунські програми для телефонів, які можна вільно придбати, встановити на пристрій користувача і спокійно за ним стежити?

- «вільне» шпигунське ПЗ
- звичайне шпигунське ПЗ
- «легальне» шпигунське ПЗ

64. Шпигунське ПЗ на телефоні може ... (виберіть 3 пункти)

- перехоплювати інформацію про всі здійснені дзвінки
- звільняти місце для себе на телефоні
- показувати вміст sms-листування
- показувати інформацію про відвідувані сайти
- встановлювати ігри на телефоні

65. Шпигунське ПЗ на телефоні може ... (виберіть 4 пункти)

- визначати Ваше місце розташування
- сканувати bluetooth чи Wi-Fi оточення
- здійснювати батьківський контроль
- включати мікрофон і записувати інформацію про все навкруги
- знімати за допомогою камери телефону оточуючу ситуацію

66. Перші мобільні віруси не можна було навіть назвати повністю вірусами, це були більше шкідливі sms, тобто на телефон користувача приходила певне sms і якщо її відкрити, тоді ...

- телефон завантажував картинки з Інтернет мережі
- телефон виконував певну не потрібну користувачу функцію
- телефон вимикався
- з телефону витиралися фотографії

67. Хробак, який розповсюджується через bluetooth, з'явився на базі ...

- Palm OS
- Windows CE
- Symbian
- Windows Mobile

68. Пізніші модифікації хробака для телефонів вже намагались ...

- вимикати телефон

- заробляти кошти зловмисникам
- завантажувати процесор
- контролювати користувачів

69. Чи існують віруси для iOS? Чи дійсно такими безпечними є iPhone та iPad у порівнянні з андроїд пристроями
    - Не існує, вони дуже захищені
    - Існують, але там є вбудована утиліта, яка захищає від усього
    - Шкідливі програми створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення

70. Які телефонні пристрої вважаються повністю захищеними?
    - На яких встановлено антивірус
    - Які працюють на базі iOS
    - Тільки пристрої з повною забороною на встановлення додаткового ПЗ є захищеними

71. Якщо користувач iPhone заразив телефон вірусом, то що йому робити?
    - Встановити антивірус і видалити загрозу
    - Користувачі iOS пристроїв змушені будуть чекати поки Apple випустить оновлення операційної системи, яке усуне вразливість
    - Встановити інше ПЗ і видалити загрозу

72. До об’єктів захисту в операційних системах відносять ... (виберіть 4 пункти)

- пам’ять
- антивіруси
- пристрої введення-виведення (наприклад, диски, принтери)
- пристрої налаштування мережі
- програми
- моніторингові програми
- дані

73. Вкрадений або втрачений iPhone – що робити? (Виберіть2 пункти)

- Піти купити новий
- Використати додаток «Знайти мій iPhone»
- Повідомити про зникнення в поліцію, вказавши серійний номер смартфона.
- Вирахувати ймовірного злочинця і самостійно відібрати телефон
- Найняти групу спеціалістів, які здійснять пошуки

74. Вкрадений або загублений Android-смартфон – що робити? (Виберіть 2 пункти)

- Піти купити новий
- Найняти групу спеціалістів, які здійснять пошуки
- У цьому випадку знадобиться застосунок під назвою «Android Device Manager» або комп’ютер із веб-браузером
- Встановити пошукове ПЗ та прослідкувати

- Повідомити про зникнення в поліцію, вказавши серійний номер смартфона

75. Рекламне ПЗ – ...

- програмне забезпечення для автоматичного відтворення відеороликів на ПК
- програмне забезпечення для встановлення спеціальних службових утиліт
- програмне забезпечення для автоматичного відтворення, відображення чи завантаження реклами на комп’ютер

76. Рекламне ПЗ працює як шкода на ...

- персональному комп’ютері
- мобільному пристрої користувача
- ПК і на мобільному пристрої користувача

77. Найчастіше рекламне ПЗ відображається у ...

- вигляді іконок прихованого програмного забезпечення
- вигляді іконок папок та файлів
- спливаючому вікні

78. Рекламне програмне забезпечення може бути безпечним?

- Так, іноді
- Ні, ніколи

79. Рекламні модулі (рекламне ПЗ) по іншому ще називають ...

- Software
- Hardware
- Adware

80. Принципи вірусної реклами – це те, що необхідно розуміти спочатку, якщо вас цікавить такий напрямок (вибрати 3 пункти)

- Орієнтація на ЦА (цільову аудиторію)
- Контент незвичайного формату
- Правильний вибір каналу розповсюдження
- Створення зручних умов для поширення контенту
- Докладно дізнатися, що таке вірусна реклама і як вона працює

81. Принципи вірусної реклами – це те, що необхідно розуміти спочатку, якщо вас цікавить такий напрямок (вибрати 3 пункти)

- Створити популярний ролик
- Ставка на емоції
- Вдало вибрати відеоплатформу
- Наявність практичної цінності
- Креативна «упаковка»

82. Переваги вірусної реклами: (вибрати 3 пункти)

- Вигода

- Масштаб
- Креативна «упаковка»
- Платформо незалежність
- Свобода від цензури

83. Етапи розробки вірусної реклами в Інтернет: (вибрати 3 пункти)

- Гарна ідея
- Реалізація
- Вибір мови програмування
- Вибір платформи
- Впровадження

84. Шпигунський програмний продукт по іншому називають

- Spyware
- Software
- Adware
- Hardware

85.Формграббер −

- шпигунська програма, яка перехоплює паролі та логіни користувача перед тим, як вони будуть передані через інтернет до сервера
- санкціоновано вживаний моніторинговий програмний продукт

- це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його

86. Keylogger – це ...

- санкціоновано вживаний моніторинговий програмний продукт
- програмний продукт (модуль) або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера
- це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його

87. За методом виготовлення Keylogger поділяють на ...

- програмні та апаратні
- людино-програмно орієнтовані
- апаратно-людино орієнтовані

88. Одним із способів захисту як від програмних так і апаратних кейлогерів є ...

- Віртуальна клавіатура
- Віртуальний аналізатор кейлогерів
- Системи моніторингу

89. Dialer – ...

- це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його
- програмний продукт (модуль) або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера

- програма, головним завданням якої є дзвінки на платні телефонні лінії з метою отримання грошей від користувача шляхом виставлення рахунків за телефонні дзвінки

90. Програма-вимагач, програма-шантажист по іншому називається ...

- Ransomware
- Adware
- Hardware

91. Програми-вимагачі – це ...

- це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його
- програмний продукт (модуль) або апаратний пристрій, що реєструє кожне натиснення на клавішу клавіатури комп'ютера
- шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв

92. Які техніки використовує програма-вимагач? (Виберіть 3 позиції)

- Шифрування диску та блокування доступу користувача до операційної системи
- Зміну операційної системи
- Оновлення ПЗ
- Блокування екрану користувача
- Шифрування даних на диску жертви

93. Суб’єктом кримінальної відповідальності за злочини, пов’язані із виготовленням шкідливого програмного чи технічного забезпечення і

посягання за допомогою нього на різного роду інформацію, яка, до речі, визнається об’єктом права власності, є особа, що досягла ...

- 14-річного віку
- 16-річного віку
- 18-річного віку

94. Рівень кримінальної відповідальності за злочини, пов’язані із виготовленням шкідливого програмного чи технічного забезпечення напряму залежить від ...

- віку злочинця
- рівня шкоди, яку було завдано винною особою
- виду шкідливого забезпечення

95. Відповідальність за створення та використання або збуту шкідливих програм передбачена (згідно законодавства України) ...

- ст. 366-1 Кримінального кодексу України
- ст. 361-1 Кримінального кодексу України
- ст. 360-1 Кримінального кодексу України

96. Створення шкідливих програмних або технічних засобів являє собою ...

- результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу.
- самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням інформаційної мережі
- оплатну чи безоплатну передачу їх у розпорядження іншої особи, а також передачу копій шкідливих програмних засобів

97.Збут шкідливих програмних або технічних засобів являє собою ...

- результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу.

- самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням інформаційної мережі

- оплатну чи безоплатну передачу їх у розпорядження іншої особи, а також передачу копій шкідливих програмних засобів

98.Розповсюдження шкідливих програм або технічних засобів являє собою ...

- результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу.

- самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням інформаційної мережі

- оплатну чи безоплатну передачу їх у розпорядження іншої особи, а також передачу копій шкідливих програмних засобів

99.Використання шкідливих програм або технічних засобів являє собою ...

- результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу.

- самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням інформаційної мережі

- оплатну чи безоплатну передачу їх у розпорядження іншої особи, а також передачу копій шкідливих програмних засобів

- дії, спрямовані на застосування цих засобів відповідно до їх властивостей і призначення

100. Відповідальність за створення, збут та розповсюдження шкідливого ПЗ чи технічних засобів передбачає ... (виберіть 3 пункти)

- або штраф
- або допомога у пошуках інших кіберзлочинців
- або виправні роботи
- або позбавлення волі
- або робота в лабораторії створення антивірусів

101. Кібершпигунство – це ...

- терористична діяльність, що здійснюється у кіберпросторі або з його використанням
- діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням
- шпигунство, що здійснюється у кіберпросторі або з його використанням

102. Кібертероризм – це ...

- терористична діяльність, що здійснюється у кіберпросторі або з його використанням
- діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням
- шпигунство, що здійснюється у кіберпросторі або з його використанням

103. Кіберрозвідка – це ...

- терористична діяльність, що здійснюється у кіберпросторі або з його використанням

- діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням

- шпигунство, що здійснюється у кіберпросторі або з його використанням

104. Українське законодавство ...

- йде попереду від європейського і американського правового регулювання питань кібербезпеки

- відстає від європейського і американського правового регулювання питань кібербезпеки

- йде в ногу з європейським і американським правовим регулюванням питань кібербезпеки

105. Чи існує єдина ефективна методика виявлення невідомого шкідливого ПЗ?

- Звичайно існує, як інакше

- Не існує

106. Методи для виявлення шкідливого ПЗ, що базуються на сигнатурах, протягом десятиліть активно використовувались для ...

- VPN

- створення правил локальної політики ПК

- антивірусного ПЗ

107. Сигнатурні методи виявлення шкідливого ПЗ ...

- точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів

- приблизні методи виявлення, які дозволяють з певною ймовірністю припустити, що файл заражений

- перехоплення даних що вводяться з клавіатури

108. Евристичні методи виявлення шкідливого ПЗ ...

- точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів

- приблизні методи виявлення, які дозволяють з певною ймовірністю припустити, що файл заражений

- перехоплення даних що вводяться з клавіатури

109. Аналіз шкідливих програм – це ...

- вивчення поведінки шкідливого ПЗ

- виконання шкідливого файлу

- один з методів перехоплення

110. Для того щоб обійти метод виявлення шкідливого ПЗ за допомогою пошуку сигнатур розробники використовують ...

- поліморфні методи

- метаморфні методи

- обфускацію коду

111. Статичний аналіз шкідливого ПЗ ...

- відстеження дій програми при виконанні, побудова її профілю

- аналіз структури бінарного файлу, його атрибутів, логічних структур, потоку виконання і даних

- використовує обфускацію коду тіла вірусу

112. Динамічний аналіз шкідливого ПЗ ...

- відстеження дій програми при виконанні, побудова її профілю
- аналіз структури бінарного файлу, його атрибутів, логічних структур, потоку виконання і даних
- використовує обфускацію коду тіла вірусу

113. Portable Executable (PE, портативний виконуваний) – формат виконуваних файлів являє собою ...

- обфускацію функцій і потоку управління
- вигляд зберігання даних або адреси виконання шкідливого коду
- структуру даних, що містить всю інформацію, необхідну PE-завантажувачу для відображення файлу в пам'ять

114. Обфускація коду – це ...

- порушення авторських прав програмістів і приховування авторства
- або заплутування чи знечитнення коду – приведення початкового коду або виконуваного програмного коду до вигляду, який зберігає його функціональність, але ускладнює аналіз, розуміння алгоритму роботи і модифікації при декомпіляції
- пропускає небажане повідомлення, які не розпізнає в ньому забороненого рядка

115. Пісочниця (комп’ютерна безпека) – це ...

- механізм для безпечного виконання програм

- програмне забезпечення для розробки ПЗ
- середовище для обфускації коду

116. Пісочниці можуть бути таких видів: ... (виберіть 3 пункти)

- Аплети
- Обфускатори
- Так звані «в’язниці»
- Віртуальні машини
- Середовища для запуску програм

117. Антивірусна програма − це ...

- комп'ютерна програма, спеціально створена для пошуку та знешкодження вірусів
- комп'ютерна програма, спеціально створена для створення та розповсюдження вірусів
- комп'ютерна програма, створена для пошуку усіх вразливостей на ПК

118. Як працювали перші антивіруси?

- Антивірус працював тільки у системі з підключенням до мережі, без її не працював
- Так як і сьогодні, оновлювалися і перехоплювали всі загрози, які здатні були перехопити
- Антивірус потрібно було запустити певною командою та вказати, що саме потрібно просканувати. Далі антивірус не працював сам по собі

119. Щоб створити сигнатуру для вірусу потрібно ...

- щоб вірус потрапив на будь який ПК
- щоб вірус уже був у лабораторії, для його детального дослідження
- щоб вірус потрапив в мережу

120. Основний недолік сигнатурного пошуку: ...

- спочатку загрозу потрібно проаналізувати
- спочатку загрозу потрібно завантажити з електронного листа
- спочатку загрозу потрібно ідентифікувати

121. Недолік евристичного аналізатору:

- вірогідність хибного спрацьовування
- складний алгоритм для реалізації
- витрата великих ресурсів для роботи

122. Поведінковий аналіз −

- точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів
- процес виявлення особливої характеристики вірусу, яка допоможе його вилікувати
- процес аналізу поведінки вірусу з метою виявлення певної притаманної шкідливої діяльності

123. Недолік поведінкового аналізатора: ...

- вірогідність хибного спрацьовування
- перевіряє програму тільки тоді коли вона уже працює
- спочатку загрозу потрібно проаналізувати

124. Основні антивірусні технології (виберіть 4 зі списку)

- Сигнатурний аналіз
- Диференціальний аналіз
- Евристичний аналіз
- Математичний аналіз
- Поведінкові аналізатори
- Схематичний аналіз
- Хмарні та репутаційні сервіси

125. Суть репутаційних технологій (до антивірусів) полягає у тому ...

- процес виявлення особливої характеристики вірусу, яка допоможе його вилікувати
- користувачі самі виявляють загрози, постійно оцінюючи нові файли
- що антивірус потрібно було запустити певною командою та вказати, що саме потрібно просканувати. Далі антивірус не працював сам по собі

126. Суть хмарних технологій (до антивірусів) полягає у тому ...

- користувачі самі виявляють загрози, постійно оцінюючи нові файли

- процес виявлення особливої характеристики вірусу, яка допоможе його вилікувати

- перевірка файлів відбувається на серверах вендорів, а не на комп'ютерах користувачів

127. Антивірусні технології не стоять на місці, сучасний розвиток йде у напрямку ...

- швидкісного реагування на шкідливе ПЗ, чи прийняття рішення білизни файлу у межах декількох хвилин

- зменшення ресурсів споживання для роботи антивірусу

- видалення знайденого шкідливого ПЗ, а не завантаження ресурсів, щоб їх лікувати

128. Чи може антивірус мати в собі додатковий інструментарій для захисту чи суто тільки знаходження шкідливого ПЗ? Якщо так, то які? (відмітьте декілька пунктів)

- Файєрвол

- Не має додаткових інструментів

- Батьківський контроль

- Механізми фільтрування веб трафіку

- Механізми віддаленого керування

129. Вам потрібно вибрати антивірус, на що ви будете звертати увагу?

- На кількість сигнатур в базі

- На швидкість оновлення антивірусу

- Використати тестування антивірусу і відгуки користувачів

- На аналізатори, що туди входять
- На функції, що виконує антивірус, чим більше тим краще

130. Яка з цих технологій антивірусного захисту була створена першою?

- Поведінковий аналіз
- Сигнатурний аналіз
- Хмарні технології
- Евристичний аналіз

131. Яка із перелічених технологій антивірусного аналізу є найбільш точною?

- Сигнатурний аналіз
- Евристичний аналіз
- Хмарні технології
- Поведінковий аналіз

132. Основним засобом захисту інформації є ...

- використання систем захисту
- використання апаратного захисту
- резервне копіювання найцінніших даних

133. Згідно видів антивірусів, сканери перевіряють ...

- оперативну або зовнішню пам’ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм

- стан BOOT-сектора, FAT-таблиці, атрибути файлів

- у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю

134. Згідно видів антивірусів, ревізори перевіряють ...

- оперативну або зовнішню пам’ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм

- стан BOOT-сектора, FAT-таблиці, атрибути файлів

- у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю

135. Згідно видів антивірусів, сторожі перевіряють ...

- оперативну або зовнішню пам’ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм

- стан BOOT-сектора, FAT-таблиці, атрибути файлів

- у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю

136. Міжмережевий екран може бути у вигляді ...

- програмного додатку

- фізичного пристрою

- фізичного пристрою чи програмного додатку

137. Міжмережевий екран призначений ...

- для контролю вхідного і вихідного трафіку на комп’ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше

- для контролю тільки вхідного трафіку на комп’ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше

- для контролю тільки вихідного трафіку на комп’ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше

138. Міжмережеві екрани виконують такі функції: (виберіть 3 пункти)

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв’язку

- багатоетапну ідентифікацію запитів, що надходять в мережу

- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі

- встановлюють двохфакторну автентифікацію

139. Міжмережеві екрани виконують такі функції: (виберіть 4 пункти)

- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні

- шифрують канал передачі даних

- контроль цілісності програмного забезпечення і даних

- економію адресного простору мережі
- приховування IP-адреси внутрішніх серверів з метою захисту від хакерів
- приховування фізичного розміщення ПК

140. Який пристрій першим реалізовував принцип апаратно- програмного брандмауера?

- Стабілізатор
- Маршрутизатор
- Мережева плата

141. Які з вказаних у списку є файєрволами? (виберіть 3 пункти)

- ZoneAlarm Free Firewall
- AIDA64
- Comodo Firewall
- GlassWire
- CCleaner

142. Рівень захищеності міжмережевих екранів оцінюється за ...

- рівнями протоколів захисту
- серверами прикладного рівня
- вказаними показниками

143. Залежно від відстеження активних сполук мережеві екрани бувають: ... (виберіть 2 пункти)

- Stateless (проста фільтрація)
- Stateful packet (SP) (фільтрація з урахуванням pesh-алфавіту)
- Stateful packet inspection (SPI) (фільтрація з урахуванням контексту)
- Statel (комбінована фільтрація)

144. Залежно від охоплення контрольованих потоків даних мережеві екрани поділяються на: ... (виберіть 2 пункти)

- Маршрутний мережевий екран
- Традиційний мережевий(або міжмережевий) екран
- Персональний мережевий екран
- Контрольований мережевий екран

145. Чи працює вбудований в ОС брандмауер стабільно?

- Так, проблем не існує
- Ні, можуть бути проблеми, які вирішуються за допомогою інструкцій

146. Чи є можливість у брандмауері Windows відновити налаштування по замовчуванню?

- Немає, кожен раз налаштовується вручну за правилами
- Немає
- Є, потрібно вибрати "відновити значення по замовчуванню"

147. Для того аби перевірити чи дійсно ваш брандмауер вас захищає потрібно ...

- його протестувати
- відновити його значення по замовчуванню
- встановити додатковий брандмауер

148. VPN перенаправляючи ваш інтернет-трафік через приватний сервер, створює зашифрований тунель, який ... (виберіть 3 пункти)

- приховує вашу особу під час користування Інтернетом
- приховує ваші хмарні сервіси, якими ви користуєтеся
- приховує ваші дані під час користування Інтернетом
- приховує вашу активність під час користування Інтернетом
- приховує яку ОС ви використовуєте на ПК

149. Чи зможуть, до прикладу, Google, Facebook або ваш інтернет-провайдер відстежувати ваші дії в мережі, якщо ви користуєтеся VPN?

- Інтернет-провайдер зможе, бо у нього всі налаштування
- Зможуть, якщо ви у VPN не вказали їх, такими, що не можуть
- Не зможуть

150. Чи зможе ваш інтернет-провайдер знизити швидкість вашого з’єднання, якщо ви використовуєте велику частку доступної пропускної здатності, коли ви користуєтеся VPN?

- зможе, бо у нього всі налаштування
- не зможе

- все залежить від VPN, яким ви користуєтеся

151. Чи зможе VPN приховати ваше фізичне місцезнаходження?

- Ні, воно приховує тільки IP-адресу
- Зможе, оскільки без знання IP-адреси не можна знайти і фізичну адресу
- Все залежить від VPN, яким ви користуєтеся

152. Які ще переваги мають VPN-сервіси? (виберіть 2 пункти)

- Здатні долати регіональні блокування по геолокації на сайтах з географічними обмеженнями
- Здатні шифрувати ваші дані на ПК
- Деякі VPN можуть блокувати непристойні сайти на які вам кортить зайти
- Деякі VPN можуть блокувати рекламу та не давати зловмисним сайтам заражати ваш пристрій шкідливими програмами та трекерами

153. Які ще переваги мають VPN-сервіси? (виберіть 2 пункти)

- Здатні шифрувати ваші дані на ПК
- VPN можуть надати вам доступ до міжнародних ігрових серверів і подолати регіональне блокування ігор
- VPN також допомагатиме долати різноманітні обмеження в мережі та фаєрволи, аби зберегти вашу свободу дій в Інтернеті
- VPN також може надати доступ до офіційних сайтів будь яких банків та виконувати деякі приховані функції

154. Чи має користування VPN якісь недоліки?

- Недоліків немає, все так як треба
- Все залежить від вибраного VPN
- Звичайно має, наприклад, може дещо знизити швидкість вашого з’єднання

155. Основні механізми забезпечення безпеки в операційній системі: ...(виберіть 4 пункти)

- Ідентифікація
- Систематизація ресурсів
- Автентифікація
- Контроль цілісності та автентичності даних
- Резервне копіювання
- Оптимізації ОС

156. Основні механізми забезпечення безпеки в операційній системі: ... (виберіть 4 пункти)

- Розмежування доступу до інформації
- Шифрування
- Оптимізації ОС
- «Firewall» (пакетний фільтр)
- Система стеження
- Аудит

- Система контролю вмісту дисків

157. Моделі управління доступом в ОС поділяються на такі категорії: ... (виберіть 4 пункти)

- операційний метод управління
- дискреційне (виборче) управління
- мандатний метод управління
- рольова модель управління
- мережева модель управління
- управління доступом на основі правил

158. Який обліковий запис користувача ОС вважається надійнішим і дозволяє нормально користуватися ПК?

- звичайний обліковий запис користувача
- обліковий запис користувач-адміністратор
- гостьовий обліковий запис

159. Для того щоб миттєво заблокувати свій ПК, якщо вам необхідно відійти від робочого місця, ви повинні натиснути: ...

- клавішу з емблемою Windows + Block
- клавішу HOME
- клавішу з емблемою Windows + L

160. Для того щоб активізувати аудит безпеки ОС потрібно зайти у ...

- Адміністрування/ аудит безпеки

- Локальну політику безпеки/ політика аудиту

- Персоналізація/ журнал аудиту

161. Мандатне керування доступом –

- розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктів на звернення до інформації такого рівня конфіденційності

- передбачає право власника або адміністратора об'єкта визначати та контролювати всіх, хто має доступ до системи або ресурсів, ґрунтуючись на ідентифікаційну інформацію про суб'єктів (ключі доступу), допущених до контрольованої системи

- передбачає розподіл функцій персоналу з урахуванням виду діяльності організації в цілому або роботи конкретного підрозділу, або при виконанні судових проектів

162. Модель рольового управління доступом –

- передбачає право власника або адміністратора об'єкта визначати та контролювати всіх, хто має доступ до системи або ресурсів, ґрунтуючись на ідентифікаційну інформацію про суб'єктів (ключі доступу), допущених до контрольованої системи

- передбачає розподіл функцій персоналу з урахуванням виду діяльності організації в цілому або роботи конкретного підрозділу, або при виконанні судових проектів

- розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктів на звернення до інформації такого рівня конфіденційності

163. Дискреційний контроль доступом −

- передбачає право власника або адміністратора об'єкта визначати та контролювати всіх, хто має доступ до системи або ресурсів, ґрунтуючись на ідентифікаційну інформацію про суб'єктів (ключі доступу), допущених до контрольованої системи

- передбачає розподіл функцій персоналу з урахуванням виду діяльності організації в цілому або роботи конкретного підрозділу, або при виконанні судових проектів

- розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктів на звернення до інформації такого рівня конфіденційності

164. Батьківський контроль можна налаштувати в ... (виберіть 2 пунтки)

- хмарному середовищі Google

- соціальній мережі Facebook

- офіційному сайті ігор-анімацій

- операційній системі Windows 10/Linux

165. Скорочено систему виявлення вторгнення /систему запобігання вторгнення позначають як ...

- IDS/IPS або (СВВ)/(СЗВ)

- IDS/IPS або (СВВТ)/(СЗТ)

- IQS/ILS або (СВВ)/(СЗВ)

166. Система виявлення вторгнення −

- програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення

- програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою

- програмна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення

167. Система запобігання вторгнення −

- програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення

- програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою

- програмна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення

168. Системи виявлення вторгнень за характером відповідної реакції можуть бути ...

- реальні, фіктивні , гібридні

- пасивні, резидентні, гібридні

- пасивні, активні, гібридні

169. Системи виявлення вторгнень за методиками аналізу можуть бути ... (виберіть 3 пункти)

- статичні

- динамічні

- евристичні
- сигнатурні
- гібридні

170. Системи виявлення вторгнень за рівнем виявлення атак можуть бути ... (виберіть 5 пунктів)

- HIPPS
- NIDS
- ROCKS
- GrIDS
- OIDS
- HIDS
- ERIDS
- FOXX

171. Найбільш популярними системами виявлення/запобігання вторгнень є...

- Snort, Suricata, Cisco Secure IDS
- Cisco Secure IDS, Secure VPN, SuperZ
- Snort, Suricata, ESET IDR

172. Архітектура IDS дозволяє розподіл її функцій між її компонентами, серед яких:

- сканери, детектори, менеджер IDS, підсистема аудиту, консоль

- сенсори, банк знань, менеджер IDS, підсистема приховувань, консоль

- сенсори, детектори, менеджер IDS, підсистема аудиту, консоль

173. Менеджер IDS ...

- контролює всі інші компоненти IDS, приймає рішення з підняття тривоги та реалізації контрзаходів

- займається безпосередньо виявленням вторгнень, ґрунтуючись на критерії виявлення

- виконують роль головної сполучної ланки IDS з обчислювальною середовищем. Вони збирають необхідну для виявлення вторгнення інформацію, фільтрують її і відсилають детекторам

174. Сенсори систем виявлення вторгнень ...

- контролює всі інші компоненти IDS, приймає рішення з підняття тривоги та реалізації контрзаходів

- займається безпосередньо виявленням вторгнень, ґрунтуючись на критерії виявлення

- виконують роль головної сполучної ланки IDS з обчислювальною середовищем. Вони збирають необхідну для виявлення вторгнення інформацію, фільтрують її і відсилають детекторам

175. Детектор системи виявлення вторгнень ...

- контролює всі інші компоненти IDS, приймає рішення з підняття тривоги та реалізації контрзаходів

- виконують роль головної сполучної ланки IDS з обчислювальною середовищем. Вони збирають необхідну для виявлення вторгнення інформацію, фільтрують її і відсилають детекторам

- займається безпосередньо виявленням вторгнень, ґрунтуючись на критерії виявлення

176. Яка різниця між IDS, IPS та брандмауером?

- немає різниці, однаково функціонують та захищають мережу
- в той час як брандмауер блокує та фільтрує мережевий трафік, IDS / IPS намагається виявити шкідливу активність та попередити адміністратора про запобігання кібератакам
- брандмауер попереджає про загрозу, система виявлення вторгнень фільтрує трафік

177. Penetration test (pentest) – ...

- симуляція кібератаки на комп'ютерні системи, мобільні застосунки та веб-додатки з метою перевірки захищеності системи
- тест комп'ютерної системи, мобільних застосунків та веб-додатків з метою виявлення функціональних помилок
- симуляція кібератаки на комп'ютерні системи з метою виявлення шпигунського ПЗ

178. Тест на проникнення допомагає ...

- виявити, наскільки та чи інша система ПК є функціонально не виконувана
- виявити, яке ПЗ потрібно встановити, щоб запобігти доступу до файлів
- виявити, наскільки та чи інша система є вразливою до хакерських атак

179. Як правильно зробити аби вбезпечити від хакерських атак, якщо ти власник компанії?

- встановити відповідне ПЗ
- використати послугу тестування на проникнення
- найняти спеціаліста з кібербезпеки

180. Встановіть порядок проведення пентесту (фази або етапи): введіть по порядку номери пунктів нижче (без пропуску), наприклад: 31254

- 1. Отримання доступу
- 2. Оцінка виявлених вразливостей
- 3. Звіт
- 4. Збір інформації про ціль
- 5. Сканування за допомогою програм

181. Які існують режими тестування? (пентесту)

- White box, Grey box, Black box
- White box, Green box, Black box
- White box-test, Grey box-test, Black box-test

182. Режим пентесту White box характеризується:

- виконавець знає про діапазон зовнішніх IP-адрес, дані збираються з відкритих джерел (найбільш наближений до дій хакера)
- виконавець має доступ до більшої кількості інформації, зокрема про структуру мережі, та отримує повний доступ до об’єкта тестування
- комбінація White Box і Black Box підходів, тобто, налаштування програми нам відомо лише частково

183. Чи можна через електронну пошту надсилати виконувані файли без архівації?

- Ні, оскільки поштові компанії самі блокують даний тип файлів
- Так, лише за умови наявності антивірусу
- Це можливо лише у разі зараження комп’ютера вірусом
- Так, потрібно лише правильно налаштувати пошту

184. Які загрози характерні для мобільних пристроїв? (Виберіть 3 пункти)

- Троянські програми
- Скімінг
- Підписки на платні сервіси
- Крадіжка коштів, через відправку смс на короткі номери

185. Який тип загроз займає друге місце за поширеністю в Україні?

- Фінансові троянці
- Файлові віруси
- Криптувальники
- Рекламні модулі

186. У чому полягають недоліки використання хмарних сервісів резервного копіювання інформації? (Виберіть 2 пункти)

- Не зручно

- Постійна потреба у Інтернет з’єднанні
- Потребує великої кількості ресурсів
- Інформацію на сервері можуть викрасти

187. Режим пентесту Grey box характеризується:

- виконавець знає про діапазон зовнішніх IP-адрес, дані збираються з відкритих джерел (найбільш наближений до дій хакера)
- виконавець має доступ до більшої кількості інформації, зокрема про структуру мережі, та отримує повний доступ до об’єкта тестування
- комбінація White Box і Black Box підходів, тобто, налаштування програми нам відомо лише частково

188. Режим пентесту Black box характеризується:

- виконавець знає про діапазон зовнішніх IP-адрес, дані збираються з відкритих джерел (найбільш наближений до дій хакера)
- виконавець має доступ до більшої кількості інформації, зокрема про структуру мережі, та отримує повний доступ до об’єкта тестування
- комбінація White Box і Black Box підходів, тобто, налаштування програми нам відомо лише частково

189. Чи є можливість замовити послугу «виконати пентест» ?

- Так, є
- Ні, немає
- Потрібно навчитися самим за допомогою відповідного ПЗ

190. Виберіть зі списку ПЗ, яке відноситься до пентесту (виберіть 3 пункти)

- NMap
- Norton AntiVirus Plus
- OpenVAS
- Avira Internet Security
- Metasploit Framework
- macOS

191. Чи є інструменти для виконання пентесту онлайн?

- Ще не розробили таких інструментів
- Є, але вони відрізняються можливостями від встановленого ПЗ
- Є, але вони всі заборонені і в нашій країні

192. Моніторингові програмні продукти – це ...

- це програмні продукти (модулі), призначені для забезпечення запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії
- це програмні продукти (модулі), призначені для забезпечення безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів
- це програмні продукти (модулі), призначені для забезпечення спостережуваності обчислювальних систем, а також такі, що дозволяють фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів – з

метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії

193. Програмні засоби, що мають властивість спостережуваності (моніторингу) можуть: ... (виберіть 3 пункти)

- визначити факти нецільового використання персональних комп'ютерів
- визначити факти використання папок та файлів
- визначити факти несанкціонованого встановлення програмного забезпечення
- проконтролювати можливість використання персональних комп'ютерів у неробочий час та виявити мету такого використання
- проконтролювати можливість використання ресурсів ПК

194. Система моніторингу ІБ дозволяє ...

- виконати інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи
- виконати інтелектуальний аналіз атак та створити запити елементів
- отримувати сотні тисяч повідомлень від безлічі користувачів кожен день

195. Технологія SIEM забезпечує ...

- отримувати сотні тисяч повідомлень від безлічі користувачів кожен день
- виконувати запити в реальному часі від мережевих пристроїв
- аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків

196. Які джерела даних використовує SIEM-система? (виберіть 3 пункти)

- Міжмережеві екрани
- Бази даних
- Антивіруси
- IDS/IPS
- Офісні додатки

197. Виберіть системи, що відноситься до моніторингу: (виберіть 2 пункти)

- Zabbix
- Creative
- SQLite
- Pandora FMS

198. Які з порад можна віднести до запобігання поширенню шкідливого ПЗ? (виберіть 3 пункти)

- Постійно оновлюйте своє програмне забезпечення
- Постійно оновлюйте своє апаратне забезпечення
- Використовуйте тільки безкоштовне ПЗ
- Використовуйте антивірусне програмне забезпечення
- Добре поміркуйте, перш ніж натискати посилання чи завантажувати будь-які дані

199. Чи можливо таке, що тільки ліцензійний антивірус може врятувати від сучасних шкідливих програм?

- проблему вирішити може тільки комплексний підхід
- можливо, адже він ліцензійний
- якщо до антивіруса добавити ще міжмережевий екран, то все вирішиться

200. Як ви думаєте чи вірне твердження «чим більше комфорту ми маємо на ПК тим менше ми захищеними є»?

- Ні, можна налаштувати комфортну роботу і з комплексним захистом
- Звичайно, бо додатковий захист потребує додаткових обмежень або налаштувань

Практичні завдання для повторення та підготовки

1. Згідно відгуків користувачів виберіть на безпечному ресурсі безкоштовну прикладну програму/утиліту для діагностики ПК (наприклад, CPU-Z чи іншу) для відображення технічної інформації про складові частини (центральний процесор, відеокарта, материнська плата, оперативна пам’ять, температура, жорсткий диск, зовнішні пристрої) персонального комп’ютера. Виконайте діагностику вашого ПК вибраною утилітою, проаналізуйте результати та зробіть висновки.

2. Оберіть/підберіть будь яке шкідливе ПЗ (наприклад, якийсь вірус або троян або інше), яке ви розумієте та знаєте як працює. Вкажіть назву, дату/період створення, принцип дії та шкоду, яку завдає дане шкідливе ПЗ. Проаналізуйте його згідно таких класифікацій: за способом розповсюдження, за метою функціонування, за метою розробки. Обґрунтуйте відповідь та зробіть висновки.

3. Оберіть/підберіть будь яке шкідливе ПЗ (наприклад, якийсь вірус або троян або інше), яке ви розумієте та знаєте як працює. Вкажіть назву, дату/період створення, принцип дії та шкоду, яку завдає дане шкідливе ПЗ. Проаналізуйте його згідно таких класифікацій: за наявністю матеріальної

вигоди, за збитком, за рівнем небезпечності дій. Обґрунтуйте відповідь та зробіть висновки.

4. Оберіть/підберіть будь який вірус. Вкажіть назву, дату/період створення, принцип дії та шкоду, яку завдає дане шкідливе ПЗ. Проаналізуйте його згідно таких ознак: за середовищем існування, за способом зараження, за особливостями використовуваних алгоритмів, за деструктивними можливостями. Обґрунтуйте відповідь та зробіть висновки.

5. Дано наступний код вірусу на мові програмування C++: вірус виключає монітор, тобто виключає живлення монітору, а через 5 секунд все повертається на місце

```
#include "stdafx.h"
#include <Windows.h>

int main()
{
    SendMessage(HWND_BROADCAST, WM_SYSCOMMAND, SC_MONITORPOWER, (LPARAM)2);

    Sleep(5000);

    SendMessage(HWND_BROADCAST, WM_SYSCOMMAND, SC_MONITORPOWER, (LPARAM)-1);

    return 0;
}
```

- проаналізуйте особливості написання;
- чим відрізняється код вірусу від коду звичайної програми;
- що, на вашу думку, потрібно знати, щоб написати шкідливе ПЗ?
- впишіть текст програми у відповідному середовищі, яке у вас встановлено та запустіть .exe файл на віртуальній машині;
- проекспериментуйте з даними у програмі;
- зробіть висновки.

6. З джерела https://www.eset.com/ua-ru/home/online-scanner/ завантажити безкоштовний онлайн сканер (він завантажиться, після натиснення на «Сканувати зараз»). Сканер не заважає роботі основного антивірусу, тому можна не хвилюватися. Налаштувати параметри періодичного сканування: вибрати день тижня та час для виконання щомісячного сканування, наприклад, вівторок, 16:00. Вибрати тип сканування **повне сканування**, просканувати та проаналізувати результати. Продемонструвати виявлені об’єкти та кількість файлів, просканованих за цей час.

7. З джерела https://www.eset.com/ua-ru/home/online-scanner/ завантажити безкоштовний онлайн сканер (він завантажиться, після натиснення на «Сканувати зараз»). Сканер не заважає роботі основного антивірусу, тому можна не хвилюватися. Налаштувати параметри періодичного сканування:

вибрати день тижня та час для виконання щомісячного сканування, наприклад, неділя, 18:00. Вибрати тип сканування **швидке сканування**, просканувати та проаналізувати результати. Продемонструвати виявлені об'єкти та кількість файлів, просканованих за цей час.

8. З джерела https://www.eset.com/ua-ru/home/online-scanner/ завантажити безкоштовний онлайн сканер (він завантажиться, після натиснення на «Сканувати зараз»). Сканер не заважає роботі основного антивірусу, тому можна не хвилюватися. Налаштувати параметри періодичного сканування: вибрати день тижня та час для виконання щомісячного сканування, наприклад, четвер, 10:00. Вибрати тип сканування **вибіркове сканування**, просканувати та проаналізувати результати. Продемонструвати виявлені об'єкти та кількість файлів, просканованих за цей час.

9. Для демонстрації безпечної роботи для дітей в мережі налаштувати «Батьківський контроль» в операційній системі. Створити обліковий запис з якого дитина буде постійно працювати. Врахувати важливий аспект – тип облікового запису, під яким дитина входитиме в систему. Для цього натискаєте на обліковий запис дитини і змінюєте на бажаний вами: стандартний користувач. **Важливо** не надавати статусу адміністратора, оскільки він дає можливість встановлювати сторонні програми, а також змінювати налаштування вашого комп'ютера. **Налаштувати такі параметри контролю: функцію моніторингу (нещодавні дії, режим перегляду веб-сторінок в Інтернеті), покупки та витрати, пошук дитини.** Зайти з облікового запису дитини та продемонструвати всі попередні налаштування контролю як це буде бачити дитина.

10. Для демонстрації безпечної роботи для дітей в мережі налаштувати «Батьківський контроль» в операційній системі. Створити обліковий запис з якого дитина буде постійно працювати. Врахувати важливий аспект – тип облікового запису, під яким дитина входитиме в систему. Для цього натискаєте на обліковий запис дитини і змінюєте на бажаний вами: стандартний користувач. **Важливо** не надавати статусу адміністратора, оскільки він дає можливість встановлювати сторонні програми, а також змінювати налаштування вашого комп'ютера. **Налаштувати такі параметри контролю: додатки, іграшки та мультимедіа, таймер роботи з пристроєм.** Зайти з облікового запису дитини та продемонструвати всі попередні налаштування контролю як це буде бачити дитина.

11. Налаштувати батьківський контроль у наявному обліковому записі Google, для безпечної роботи дитини у мережі, через додаток Family Link.

Налаштувати такі можливості: додатки на контрольованому пристрої, місцезнаходження пристрою, час використання пристрою, фільтри в Google Chrome, пошук Google і Google Play. Зайти з облікового запису дитини та продемонструвати всі попередні налаштування контролю та як це буде виглядати. Проаналізувати чи зможе дитина сама вимкнути батьківський контроль.

12. Провести експеримент з використанням методу соціальної інженерії. Відправити повідомлення 10-м своїм друзям чи знайомим з текстом "Привіт, знаю, що зараз не актуально :-) Просто глянь! Цікаво ж як!!!" і посиланням (посилання вибрати на будь який безпечне джерело). Можна текст інший, то тільки приклад. Але текст повинен бути згідно рекомендацій, щоб зачепити користувача на «гачок». Продемонструвати скріни відповідей. Проаналізувати реакцію та дізнатися чи переходили ваші знайомі за посиланням. Зробити висновки про дотримання інформаційної гігієни.

13. Виконати експеримент за методом соціальної інженерії «Листи від банків»:
    - створити поштову скриньку на будь якому доступному для цього ресурсі, назвати її так, щоб отримувач думав, що лист надсилає Приватбанк;
    - сформулювати лист таким чином, щоб користувач думав, що «потрібно уточнити інформацію» для банку, попросити надіслати зворотний лист з уточненими даними;
    - надіслати листи на поштові скриньки користувачів подані викладачем;

    Проаналізувати отриману інформацію та листи-відповіді. Зробити висновки щодо дієвості даного методу соціальної інженерії.

14. Провести визначення прихованого майнінгу. Для цього можна використати декілька способів:
    - диспетчер задач (обґрунтувати, на що там потрібно подивитися та як розуміти результат);
    - утиліта, яка перевіряє температуру пристрою, рівень використовуваної енергії, звернути увагу на швидкість запуску програм (обґрунтувати результат);
    - пошук у кодах сторінок сайтів слова «coin».

    Проаналізувати отриману інформацію та дати чітку відповідь про присутність прихованого майнінгу на ПК та у кодах сторінок сайтів. Обґрунтувати за що відповідають наступні розширення у браузері: ScriptBlock, NoCoin і MinerBlock.

15. Охарактеризуйте, що таке фінансовий номер телефону та яка різниця між передплаченим та контрактним мобільним зв'язком (коли користувач в більшій небезпеці, коли ні). Опишіть, що потрібно зробити для перевипуску мобільної карти (алгоритм дій) та як це буде виглядати для користувача. Виділіть моменти на що потрібно звернути увагу та які дії має виконати користувач терміново. Як відновити сім-карту? Наведіть поради та правила кібергігієни, щоб такі дії зловмисників унеможливити або запобігти такому.

16. Що робити в разі втрати гаджета? Перерахуйте, що може зробити шахрай, якщо викрав ваш гаджет. Сформулюйте правила для захисту гаджету при викраденні. Що таке послуга «знайти телефон»? Продемонструйте як її встановити. Що таке IMEI, як він може допомогти? Які державні органи можуть допомогти? Що таке «семпл»?

17. Як відбувається мобільний (телефонний) фішинг? Наведіть приклади повідомлень, які намагаються «зачепити на гачок». Які підказки допоможуть виявити фішингове повідомлення? Як боротися з фішингом на телефоні? Чи користуєтесь антивірусом для телефону, якщо ні то продемонструйте де його взяти. Який з цих сайтів є фішинговий: https://www.olx.ua чи https://novaposhta.at? Обґрунтуйте відповідь.

18. Коли телефонують шахраї (вішинг): що це таке та як відбувається? Наведіть приклади розмов при вішингу. Яких чітких правил потрібно дотримуватися, щоб не попастися на вішинг? Як розпізнати різні сценарії зловмисників та вберегти персональну інформацію? Від кого можуть телефонувати (представлятися)? Наведіть приклади програмного забезпечення для перевірки та ідентифікації номеру як шахрайського. Як воно працює та до чого повинне мати доступ?

19. Чи можна рекламне ПЗ (Adware) полікувати чи його потрібно видаляти? Відповідь обґрунтуйте. Щоб заблокувати рекламу та позбутися її назавжди, необхідно очистити сам браузер. Продемонструйте очищення вашого браузера відповідно до інструкцій (з врахуванням часу). Опишіть інший шлях блокування реклами, якщо очищення браузера не допомогло. Яку конфіденційну інформацію зчитує з ПК рекламне ПЗ (перерахуйте)?

20. Опишіть поняття вірусного маркетингу та найпоширеніші його технології (види). Детально охарактеризуйте кожну технологію. Продемонструйте лайфхаки для створення вірусного контенту в Instagram або Facebook.

Продемонструйте приклади вірусного відео (реклами) та вкажіть його особливості. Вкажіть плюси та мінуси вірусного маркетингу. Ч навчилися ви розрізняти коли присутній вірусний маркетинг? Зробіть висновки.

21. Які типи шпигунського ПЗ ви знаєте? Охарактеризуйте кожен тип. Звідки береться шпигунське ПЗ на ПК чи на гаджет? Перерахуйте попереджувальні ознаки шпигунського ПЗ. Охарактеризуйте ПЗ Gridinsoft Anti-malware (https://gridinsoft.ua/antimalware) та його особливості. Продемонструйте роботу Anti-malware (безкоштовний пробний період 6 днів). Вкажіть функції, які може виконувати ПЗ, виконайте швидке сканування, проаналізуйте результати.

22. Для чого потрібні розширення для браузерів такі як NoScript та AdBlock? Охарактеризуйте відгуки користувачів та проблеми, які можуть виникати при роботі з цими розширеннями. Продемонструйте налаштування та роботу NoScript або AdBlock.

23. Дослідіть та охарактеризуйте статті 361, 361-1, 361-2, 362 КК України. Поясніть чим вони відрізняються та наведіть приклади коли застосовуються. Опишіть відповідальність за порушення. Визначіть поняття: створення шкідливого ПЗ, використання шкідливого ПЗ, розповсюдження шкідливого ПЗ, збут шкідливого ПЗ. Опишіть орієнтовний алгоритм дій при порушенні статті 361-1 та можливий порядок оскарження рішення згідно законодавства України.

24. Користуючись пошуковою системою знайдіть приклади виявлення:
    - створення шкідливого ПЗ;
    - використання шкідливого ПЗ;
    - розповсюдження шкідливого ПЗ;
    - збуту шкідливого ПЗ.

    Приклади можуть поєднувати дії. Проаналізуйте випадки злочинів, вкажіть чи покарані злочинці та суми збитків, які вони завдали.

25. Що таке пісочниця та для чого вона необхідна? Переглянути відеоролик “Налаштування пісочниці” за посиланням https://www.youtube.com/watch?v=8u1p_q47wyc&ab_channel=AlexanderAdamov та:
    - охарактеризувати 3 підходи: віртуальна машина, реальна машина, гібридний;
    - описати алгоритм налаштування;
    - дослідити невідомі поняття у відео, якщо такі були.

26. Охарактеризувати та дослідити методики виявлення шкідливих програм, обґрунтувати переваги та недоліки:
    - сигнатурний аналіз або підхід, заснований на аномаліях;
    - евристичний підхід (в загальному);
    - статичний аналіз (StaticApproach);
    - динамічний аналіз (Dynamic Approach);
    - гібридний підхід (Hybrid Approach);
    - підходи, що засновані на візуалізації.

    На основі отриманих даних зробити висновки про методи виявлення шкідливих програм.

27. Опишіть та обґрунтуйте детальний алгоритм підготовки ПК до вірусної чи іншої атаки з боку шкідливого ПЗ. Обов’язково має бути вказано процес створення системної флешки, всі можливі перевірки. Створіть таблицю, у якій вкажіть все необхідне програмне забезпечення, яке допоможе вам при відновленні працездатності комп'ютера (передбачити випадок зіпсованої файлової системи, тестування всіх підсистем комп’ютера, на виявлення несправності апаратури та ін.) та обґрунтуйте доцільність та використання кожного.

28. Згідно класифікації антивірусів (сканери, ревізори і т.д.) дослідити які з антивірусів до якої групи належать. Знайти до кожної групи по декілька, якщо антивірусне ПЗ об'єднує функції груп, то так і вказати. Назва антивірусу – група. Наприклад, антивірусне ПЗ ADinf – ревізор. Дослідити які методи пошуку шкідливого ПЗ використовує вибране вами антивірусне ПЗ (евристичний аналіз чи сигнатурний чи інший і т.д., чи усі).

29. Робота з антивірусним програмним забезпеченням: налагодити програму, організувати захист комп’ютера від шкідливого ПЗ (проаналізувати встановлене на вашому ПК, не вбудоване в операційну систему). Продемонструвати та прокоментувати всі можливості та модулі. Які методи пошуку використовує даний антивірус? Чи є якісь цікаві додаткові можливості? Як видає результат та що можна проаналізувати за результатом?

30. Опишіть різницю між хмарним та традиційним антивірусом. Детально визначне переваги та недоліки хмарного та традиційного антивірусу. Наведіть приклад хмарного антивірусу. Що таке репутаційні технології, яка їх особливість і як можна використовувати?

31. Робота з міжмережним екраном:
- детально охарактеризувати функції та можливості **вашого** міжмережного екрану (брандмауера, вбудованого в ОС);
- продемонструвати можливі налаштування та як це буде впливати на його роботу?
- для демонстрації, на ваш розсуд, створити декілька нових правил та показати їх, обґрунтувати для чого вибрані такі правила;
- продемонструвати як працюють задані вами правила;
- що можна налаштувати в розділі «Обслуговування та безпека»?;
- продемонструвати як переглянути журнал звітів про стабільність.

Зробіть висновки про необхідність міжмережного екрану.

32. Як можна перевірити чи добре працює міжмережевий екран? Перевірити **якість** роботи вашого **вашого** міжмережного екрану. Вибрати для перевірки певний спосіб та продемонструвати. Одним зі способів є тестування міжмережного екрану. Охарактеризуйте детально, що можна побачити при тестуванні. Для виконання завдання оберіть:
- або відповідне тестуюче програмне забезпечення згідно відгуків користувачів або з інших причин;
- або використайте спеціальний сайт;
- або застосуйте сканери вразливостей та проскануйте внутрішній діапазон IP-адрес.

Покажіть результати перевірки та зробіть висновки.

33. Чому важливо у щоденній роботі використовувати саме обліковий запис без прав адміністратора? Поясніть. Покажіть всіх вже існуючих в ОС Windows користувачів, їх роль в системі, а також статус. Як можна змінити параметри існуючого облікового запису: пароль, малюнок, права. Створіть новий обліковий запис користувача у вашій ОС. Продемонструйте надання прав та можливостей новому користувачу. Покажіть роботу в створеному обліковому записі. Чи діють вказані вами обмеження доступу? Як видалити непотрібний обліковий запис?

34. Визначити правила коли пароль вважається надійний. Дати відповідь на питання:
- як перевірити чи надійний пароль?
- як згенерувати надійний пароль, за допомогою чого?
- що таке менеджер паролів та його функції, приклади менеджерів.

Продемонструйте виконання кожного пункту.

35. Особливості роботи системи виявлення вторгнень Snort. Дана система виявлення вторгнень працює із попередньо заданими шаблонами

шкідливого трафіку, так званими правилами (rules), які дозволяють визначити, який трафік у мережі є шкідливим, а який – ні. Для демонстрації роботи системи виконати наступні завдання:

- описати особливості процесу встановлення системи Snort;
- написати загальний синтаксис правила;
- продемонструвати створення своїх правил;
- запустити режим виявлення вторгнень, продемонструвати результати;
- написати загальний формат написання контекстних правил (підключення препроцесорів);
- продемонструвати результат сканування портів;
- продемонструвати результат тесту на безпеку.

36. Дослідження тестування на проникнення (pentesting):
    - детально описати етапи проєкту з оцінки захищеності;
    - детально описати, що входить у: виявлення, висновки, рекомендації;
    - коротко описати відомі вам методології тестування на проникнення (назва, суть, особливості, функції та ін.)

37. Сканування мереж за допомогою програми NMAP (інструмент для тестування на проникнення):
    - назвати усі методи сканування, що дозволяє здійснювати NMAP;
    - детально описати кожен метод сканування (наприклад, ping-сканування, віконне сканування і т.д.).

38. Сканування мереж за допомогою програми NMAP (інструмент для тестування на проникнення):
    - продемонструвати сканування TCP-портів цілі “повним перебором” з використанням connect();
    - вибрати будь які два сканування та продемонструвати:
        - ✓ сканування TCP SYN
        - ✓ сканування Stealth FIN
        - ✓ сканування Xmas tree
        - ✓ Null-сканування
        - ✓ сканування з використанням FTP
        - ✓ сканування UDP-портів

39. Тестування на проникнення за допомогою ПЗ Metasploit Framework:
    - які два варіанти роботи має вказане ПЗ?
    - опишіть основні команди *msfconsole* (команда – дія);

- у консолі msfconsole ввести команду search dcerpc для пошуку всіх експлойтів, продемонструвати виведення;
- продемонструвати іншу (підготовлену) роботу (з використанням модулів) даного ПЗ на ваш вибір з поясненням.

40. Продемонструвати роботу декількох онлайн-інструментів Pentest для розвідки та пошуку експлойтів:
    - дослідження домену, який може виявити субдомени, пов’язані з цільовим доменом;
    - перевірити, чи є компанія вразливою до фішингу, потрібно знайти адреси електронної пошти працівників, які працюють у цільовій компанії;
    - виявлення прихованих файлів і каталогів.

41. Дослідження роботи системи Splunk:
    - коротко описати особливості SIEM;
    - призначення системи Splunk;
    - описати принцип роботи системи;
    - детально охарактеризувати усі функції системи;
    - огляд Splunk Enterprise Security: панель моніторингу безпеки, аналіз інцидентів, дії загроз, засоби для розслідування, візуальні таблиці та ін.;
    - опишіть можливість створювати нові додатки засобами Splunk;
    - що таке SPL запити?

42. Продемонструвати роботу з Kaspersky Safe Kids:
    - блокування шкідливого контенту;
    - керування розкладом та тривалістю користування пристроєм;
    - перегляд місцезнаходження та рівня заряду акумуляторної батареї пристрою;
    - моніторинг активності в соціальних мережах.

43. Надати практичні поради для захисту вашого ПК та мобільного пристрою від шкідливого ПЗ. Вказати чітко важливі, на вашу думку поради, та розмістити їх у списку від найважливіших до менш важливих. З детальним поясненням чому так, а не інакше. Окремо для ПК, окремо для мобільного пристрою.

СПИСОК СИКОРИСТАНИХ ДЖЕРЕЛ

1. Діагностика. URL: https://biblprog.org.ua/ua/diagnostic/
2. Шкідливі програми. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/
3. Типи шкідливих програм: від Trojan до Rootkit. URL: https://zillya.ua/tipi-shkidlivikh-program-vid-trojan-do-rootkit
4. Класифікація шкідливого програмного забезпечення. URL: https://studfile.net/preview/5206321/
5. Онлайн-курс «Основи інформаційної безпеки». URL: https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about
6. Троянські віруси і програми: у чому їх небезпека. URL: https://bitdefender.ua/blog/troyanskie-virusy-i-programmy-v-chem-ikh-opasnost/
7. Типи шкідливого ПЗ: троянські програми. URL: https://zillya.ua/tipi-shkidlivogo-pz-troyanski-programi
8. Категорії шкідливих програм. URL: https://zillya.ua/virus/trojan_f
9. Стелс-віруси. URL: https://studfile.net/preview/3904449/page:34/
10. Основні Інтернет-загрози. URL: http://safe-city.com.ua/osnovni-internet-zagrozy/
11. Інтернет-залежність. URL: https://healthcenter.od.ua/psyhichne-zdorovya/internet-zalezhnist/
12. Інтернет-загрози для дітей. Які вони та як їх уникнути? URL: https://legalaid.gov.ua/novyny/internet-zagrozy-dlya-ditej-yaki-vony-ta-yak-yih-unyknuty/
13. Серіал для батьків «Безпека дітей в інтернеті»/ Дистанційний курс. URL: https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey
14. Соціальна інженерія або маніпуляції свідомістю. URL: https://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu
15. Прихований майнінг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/skrytyy-mayning/
16. Конспект лекції: Загрози для мобільних пристроїв. URL: https://valeriy67.gitbooks.io/-/content/chapter_4.html
17. Безпека смартфона: рекомендації щодо забезпечення захисту телефона. URL: https://eset.ua/ua/blog/view/24/bezopasnost-smartfona-rekomendatsii-po-obespecheniyu-zashchity-telefona
18. Рекламне ПЗ. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/reklamnoye-po/

19. Принципи створення вірусної реклами. URL: https://t1.ua/special/60289-pryntsypy-stvorennya-virusnoyi-reklamy.html
20. Типи та приклади шпигунського ПЗ. Мобільні шпигунські програми. URL: https://gridinsoft.ua/spyware
21. Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
22. Кримінальні правопорушення у сфері використання комп'ютерів та комп'ютерних мереж. URL: http://surl.li/fihzf
23. CyFra - Тестування безпеки та симуляція кібератак із використанням ML. URL:https://www.youtube.com/watch?v=FrG640NtCCE&ab_channel=AlexanderAdamov
24. Сучасні методи виявлення шкідливих програм. URL: https://drive.google.com/file/d/1EpD2_xxEk3RANieYEUfNZW8IqvoKEHFU/view
25. Огляд статичних методів аналізу зловмисного програмного забезпечення. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1179859.pdf
26. Ільїн М. І. Зворотна розробка та аналіз шкідливого програмного забезпечення курс лекцій. URL: https://infosec-kpi.in.ua/assets/files/re_slides.pdf
27. Що таке пісочниця? URL: http://surl.li/fiifr
28. Антивірусні технології: в пошуках панацеї. URL: https://zillya.ua/antivirusni-tekhnologi%D1%97-v-poshukakh-panatse%D1%97
29. Міжмережевий екран. URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran
30. Поняття та різновиди міжмережевих екранів. URL: https://texnogid.biz.ua/wi-fi/bezpeka/mizhmerezhevyj-ekran.html
31. Основні принципи роботи та налаштування міжмережевих екранів. URL: https://www.chernigov.ua/news/internet/2594-osnovni-
32. Що таке VPN, і навіщо він вам у 2023. URL: http://surl.li/fiimz
33. Моделі та методи контролю доступу. URL: https://worldvision.com.ua/modeli-i-metody-kontrolya-dostupa-chto-vam-podkhodit/
34. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf
35. 10 найкращих систем виявлення вторгнень 2021 рейтинг. URL: https://uk.myservername.com/top-10-best-intrusion-detection-systems
36. Тест на проникнення. URL: https://www.pentest.com.ua/lp/

37. Секрети кібербезпеки: Що таке пентест і навіщо він потрібен компаніям? URL: https://eba.com.ua/sekrety-kiberbezpeky-shho-take-pentest-i-navishho-vin-potriben-kompaniyam/
38. Сканування TCP/IP мереж за допомогою програми NMAP. URL: https://studfile.net/preview/9649955/
39. Як користуватися Metasploit Framework: можливості, інструкція по застосуванню. URL: https://what.com.ua/iak-koristyvatisia-metasploit/
40. Системи моніторингу та управління безпекою. URL: http://integritysys.com.ua/security/siem/
41. Що таке SIEM система? URL: https://ua.softlist.com.ua/articles/chto-takoe-siem-sistema/

УДК 004.4(072)
Г 54

Електронне мережне навчальне видання

Л. Я. Глинчук

ДІАГНОСТИКА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: МЕТОДИЧНІ ВКАЗІВКИ ДЛЯ ПІДГОТОВКИ ДО ПІДСУМКОВОГО ОЦІНЮВАННЯ

для студентів спеціальності 125 Кібербезпека
першого (бакалаврського) рівня

Друкується в авторській редакції