**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії***

**ЛАБОРАТОРНА РОБОТА № 4**

з курсу

***«Безпека програм та даних»***

**ТЕМА: Захист програмного забезпечення.**

**Студент : Трембіцький Нікіта**

**Група : 31ІПЗ**

**Факультет : Інформатики**

**Викладач : Галицький О.В.**

Київ 2019

1. **1.** За допомогою пошукової системи глобальної мережі Інтернет знайти та описати не менше п’яти вразливостей ОС MS Windows (версію ОС вибрати з списку відповідно до порядкового номеру в журналі): Windows Vista:



* + MS09-001: Уразливості в протоколі SMB роблять можливим віддалене виконання коду. Зловмисник, який скористався нею, зможе встановлювати програми, переглядати, змінювати, видаляти дані або створювати нові облікові записи з необмеженими повноваженнями. Стандартні параметри конфігурації брандмауера дозволяють захистити мережу від атак з-за меж середовища організації. Microsoft в 2009 році визначив рівень цієї небезпеки як «критичний» для Microsoft Windows 2000, Windows XP і Windows Server 2003 (для Windows Vista і Windows Server 2008 - «середній») і випустив оновлення для системи безпеки, яке усуває уразливості шляхом перевірки полів в SMB-пакетах
  + MS09-050 (порт 445). Ця вразливість в протоколі SMBv2 роблять можливим віддалене виконання коду, якщо зловмисник відправить на комп'ютер, на якому виконується служба сервера, спеціально створений SMB-пакет. Microsoft в 2009 році визначив рівень цієї небезпеки як «Критичний» і випустив оновлення, що усуває уразливості за рахунок виправлення перевірки полів в пакетах SMBv2, виправлення способу обробки значення команди в SMB-пакеті, а також виправлення способу синтаксичного аналізу SMB-пакетів.
* MS11-030 (порт 5355): вразливість при вирішенні DNS робить можливим віддалене виконання коду, зловмисник отримує доступ до мережі, а потім створює програму для розсилки цільовим системам спеціально створених широкомовних запитів LLMNR. Microsoft в 2011 році визначив рівень цієї небезпеки як «критичний» і випустив оновлення, виправляє спосіб обробки клієнтом DNS запитів.
* MS12-020 (порт 3389): уразливості в віддаленому робочому столі роблять можливим віддалене виконання коду, якщо зловмисник відправляє вразливою системі послідовність спеціально створених пакетів RDP. (За замовчуванням протокол віддаленого робочого стола (RDP) відключений у всіх операційних системах Windows, тобто системи, на яких не було включено RDP, не схильні до даної уразливості). Microsoft в 2011 році визначив рівень цієї небезпеки як «критичний» і випустив оновлення, змінює спосіб обробки пакетів в пам'яті протоколом RDP і спосіб обробки пакетів службою RDP.

1. За допомогою пошукової системи глобальної мережі Інтернет знайти та описати не менше п’яти вразливостей ОС Linux (версію ОС вибрати з списку відповідно до порядкового номеру в журналі): Mandriva:



1. Недоробка, що дозволяє обійти обмеження open\_basedir і отримати доступ до зовнішніх файлів;
2. Вразливості в DRM-модулі для відеокарт i915. Відправка спеціально оформленого запиту через i915 GEM ioctl потенційно може призвести до виконання коду локального зловмисника з привілеями ядра системи.
3. В реалізації функції "snd\_ctl\_new ()" з звукової підсистеми Linux-ядра знайдено цілочисельне переповнення, використовуючи яке локальний зловмисник може викликати крах ядра або потенційно організувати виконання коду з підвищеними привілеями через відправку спеціально підготовленого запиту до пристрою "/ dev / snd / controlC \*.
4. Вразливість, що дозволяє локальному зловмисникові виконати код з підвищеними привілеями через відправку спеціально оформленого запиту до RDS-сокету.
5. Вразливість, пов'язана з некоректним форматуванням рядка в розширенні phar і дозволяє отримати доступ до областей пам'яті PHP-інтерпретатора або здійснити свій код при обробці спеціальним чином оформленої посилання "phar :/ /";
6. За допомогою пошукової системи глобальної мережі Інтернет знайти та описати не менше п’яти вразливостей офісного пакету MS Office XP.



1. Діра в захисті, виявлена в поштовій програмі Outlook XP, дозволяє запускати програмний код, вбудовані в e-mail без відома користувача. Друга вразливість була виявлена в засобі створення електронних таблиць MS Excel. Ця діра в захисті може бути використана разом з уразливістю в Outlook для приміщення виконуваних файлів в папку автозапуску системи, що може призвести до отримання повного контролю над системою.
2. Уразливість виникає через помилки в перевірці вхідних даних при обробці Word файлу. Експлуатування уразливості призведе до використання неініціалізованих покажчика.
3. Уразливість виникає через помилки в перевірці вхідних даних при обробці Word файлу. Експлуатування уразливості призведе до псування пам'яті на цільовій системі.
4. Уразливість виникає через помилки в перевірці вхідних даних при обробці значень індексу Word файлу. Експлуатування уразливості призведе до псування пам'яті на цільовій системі.
5. Уразливість виникає через помилки в перевірці вхідних даних при обробці певних значень, що повертаються в Word файлі. Експлуатування уразливості призведе до псування пам'яті на цільовій системі.
6. За допомогою пошукової системи глобальної мережі Інтернет знайти та описати не менше п’яти вразливостей офісного пакету OpenOffice 2.



1. Уразливість виникає через помилки в перевірці вхідних даних в бібліотеці libwpd. Атакуючий може обманним чином змусити користувача відкрити зловмисний WordPerfect документ, що призведе до виконання довільного коду.
2. Уразливість виникає через помилки в перевірці вхідних даних в аналізаторі StarCalc. Атакуючий може обманним чином змусити користувача відкрити зловмисний документ, що призведе до виконання довільного коду.
3. Уразливість виникає через помилки в обробці мета символів шелл. Атакуючий може обманним чином змусити користувача відкрити спеціально складений документ і перейти по зловмисної посиланням, що призведе до виконання довільних шелл команд.
4. Уразливість виникає через помилки в перевірці вхідних даних при обробці EMF, Quattro Pro, і OLE файлів. Атакуючий може передати спеціально сформовані файли, що призведе до переповнення динамічної пам'яті і виконання довільного коду.
5. Уразливість виникає через помилки в перевірці вхідних даних при обробці ODF текстових документів, що містять спеціально складені XForms. Атакуючий може передати спеціально сформовані файли, що призведе до псування пам'яті і виконання довільного коду.
6. За допомогою пошукової системи глобальної мережі Інтернет знайти та описати не менше п’яти вразливостей браузерів (окремо для Internet Explorer 8



1. Уразливості, що дозволяють зловмисникові отримати доступ до системи. Найчастіше дана уразливість зводиться до виконання машинного коду, створеного зловмисником. Найбільш розповсюдженим різновидом з даної категорії є переповнення буфера, яке призводить до зриву стека і до виконання програмного коду, сформованого атакуючим. Крім того, за статистикою автора, нерідкі уразливості, засновані на некоректної обробки CHM-файлів через протоколи ms-its (ms-itss, its, mk: @MSITStore) - дана методика часто застосовується для впровадження на комп'ютер користувачів троянських програм і SpyWare-компонентів .
2. Уразливості, що призводять до створення DoS. Під DoS в даному випадку мається на увазі будь-який збій в роботі Internet Explorer, починаючи від його аварійного завершення і зависання і закінчуючи значними витратами ресурсів і зниженням продуктивності системи в цілому. Найтиповіша реалізація - переповнення буфера (тільки в разі DoS досить простого зриву стека), шкідливі скрипти. Найпростішою демонстрацією DoS може служити HTML-файл виду:

<Body onload = "window ();">

</ Body>

Відкриття такого файлу в Internet Explorer 6.0 призводить до аварійного завершення роботи браузера.

1. Обхід налаштувань безпеки, заданих для поточного домену. Internet Explorer використовує так звану доменну модель забезпечення безпасность (Cross-Domain Security Model), основна ідея якої полягає в тому, що операції з даними, відкритими у вікні одного вузла, недоступні з боку іншого. Файлова система локального комп'ютера розглядається як домен, а отже, при порушенні доменної безпеки можна отримати доступ до локальних файлів. Одним з методів обходу налаштувань безпеки є застосування тега IFRAME - це плаваючий фрейм, який розміщується в web-сторінці аналогічно зображенню; в реалізації підтримки IFRAME в IE різних версій відомий ряд вразливостей, які дуже широко експлуатувалися (і експлуатуються) поштовими хробаками.
2. Спуфінга. Найбільш поширені форми спуфинга - відображення в поле «адреса» Internet Explorer такої адреси, яка не збігається з адресою завантаженого сайту (це називається URL-спуфинг); відображення спливаючих вікон (які, з точки зору користувача, належать переглядається в браузері сторінці (див. приклад http://secunia.com/multiple\_browsers\_ dialog\_origin\_ vulnerability\_test /, в якому відкривається вікно IE з сайтом www.google.com, а потім виводиться діалогове вікно, візуально належить даній сторінці); модифікація заголовка вікна або даних в панелі статусу.
3. Міжсайтовий скриптинг. Міжсайтовий скриптинг (Cross-Site Scripting, CSS) полягає в тому, що в завантажену web-сторінку впроваджується сторонній код, створений атакуючим. Як правило, подібний вид атаки можливий через некоректну обробки параметрів запиту на стороні сервера (в цьому випадку на сервер передається особливим чином сконструйований запит) або через уразливості самого браузера (наприклад, відома уразливість в DHTML Edit ActiveX). В результаті таких атак в контексті завантаженої Web-сторінки виконується шкідливий скрипт, який може застосовуватися, зокрема, для крадіжки Cookies, модифікації вмісту Web-сторінки, перехоплення сесії. Детальний опис уразливості в DHTML Edit ActiveX можна знайти за адресою http://secunia.com/advisories/13482/, а за адресою http://secunia.com/internet\_explorer\_ cross-site\_scripting\_vulnerability\_test / розміщений тестовий експлоїт, який демонструє застосування даної уразливості).

**Opera 9**



1. Уразливість виникає через помилки в перевірці вхідних даних. Атакуючий може зробити XSS напад на цільову систему.
2. Уразливість виникає через помилки в перевірці вхідних даних при обробці TLS сертифікатів. Атакуючий може передати спеціально сформовані дані, що призведе до виконання довільного коду.
3. Уразливість виникає через помилки в редагуванні тексту Rich при використанні режиму designMode. Атакуючий може зробити XSS напад на цільову систему.
4. Уразливість виникає через помилки в перевірці вхідних даних при обробці растрових графічних зображень. Атакуючий може отримати доступ до вмісту довільних ділянок пам'яті.

**Mozilla Firefox 9**



1. Уразливість існує через невідомих помилок. Віддалений користувач може викликати пошкодження пам'яті і виконати довільний код на цільовій системі.

2. Уразливість існує через помилку при обробці вкладеного фрейма. Віддалений користувач може обійти політику навігації фреймів і за допомогою атрибута імені здійснити фішинг атаку.

3. Уразливість існує через помилку в методі AttributeChildRemoved () при видаленні вузлів child з вузла nsDOMAttribute. Віддалений користувач може виконати довільний код на цільовій системі.

4. Уразливість існує через помилку в реалізації перевірок безпеки XPConnect при виклику недовірених об'єктів. Віддалений користувач може здійснити атаку міжсайтового скриптинга.

5. Уразливість існує через помилку в методі mImageBufferSize () при кодуванні зображень в image / vnd.microsoft.icon. Віддалений користувач може розкрити важливі дані на цільовій системі.

**Google Chrome 16.**



1. Використання після звільнення уразливості в Google Chrome 17.0.963.66 і більш ранніх версій дозволяє віддаленому зловмисникові обійти механізми захисту DEP і ASLR і виконати довільний код, за допомогою невизначених векторів, як показано на VUPEN під час змагань на Pwn2Own CanSecWest 2012 року, зверніть увагу: первинний постраждалий продукт може бути уточнений пізніше; він не був ідентифікований дослідником, який нібито заявив, що «це насправді не має значення, якщо це третя сторона коду.»
2. Стан гонки в Google Chrome 16 дозволяє віддаленому зловмисникові виконати довільний код за допомогою векторів, які викликають збій процесу корисності.
3. Google Chrome 16 неправильно обробляти SSL сокетов, що дозволяє віддаленому зловмисникові виконати довільний код або викликати відмову в обслуговуванні (корупційного пам'яті) за допомогою невизначеного вектора.
4. Google Chrome 16, перш ніж на Windows, і не виконує жодних дані вершини, яка дозволяє віддаленому зловмисникові виконати довільний код або викликати відмову в обслуговуванні (корупційного пам'яті) за допомогою невизначеного вектора.
5. Підсистема розширення в Google Chrome 16 перед тим не правильно обробляти історію навігації, яка дозволяє віддаленому зловмисникові виконати довільний код, використовуючи «універсальний XSS (UXSS)» питання.
6. За допомогою пошукової системи глобальної мережі Інтернет знайти, при необхідності встановити (встановлювати програмні засоби слід на віртуальну машину) та дослідити програмні засоби для виявлення вразливостей захисту в програмах (приклади див. в теоретичному матеріалі). Описати 2-3 програмних засоби за наступною схемою:



* + Назва - AVAST, версія - 12.3.2280, автори - AVAST Software.
  + Ліцензія (спосіб розповсюдження) – 30 днів/ ліцензія.
  + Технічні характеристики програмного засобу та мінімальні вимоги до програмноапаратних засобів - Windows XP—10 (32/64-bit), Linux, Macintosh, Palm OS, Windows Server Edition, Android
  + Режим роботи виконання на боці клієнта.
  + Наявність Інтернет-підтримки – оновлення.
  + Мова інтерфейсу - Багатомовний (45 мовних пакетів).
  + Особливості управління об’єктами інтерфейсу програми - управління відбувається за допомогою миші та клавіатури, присутні гарячі клавіши, легкий у використанні.
  + Позитивні особливості програми:
  1. Відалення шпігунського програмного забезпечення (англ. Spyware) з комп'ютера.
  2. Можлівість встановлення пароля на зміну настройок програми.
  3. Багатомовній інтерфейс, підтримка 45 мов.
  4. Голосові ПОВІДОМЛЕННЯ при віявленні шкідлівої програми и при успішному оновленні вірусної бази даних. До п'ятої Версії вікорістовувався чоловічий голос. Починаючі з п'ятої - жіночий.
  + Можливі застосування програмного засобу.

Екран файлової системи — основний компонент сканера в реальному часі. Відстежує всі локальні операцій з файлами та папками на комп'ютері. Екран пошти — відстежує весь трафік програм для роботи з електронною поштою і сканує всі листи до того, як вони потраплять на комп'ютер, таким чином запобігаючи можливій шкоді. Здійснює перевірку трафіку по протоколах POP, SMTP, IMAP і NNTP.



* + Назва - Kaspersky Anti-Virus, версія - 16.0.0.614, автори - Лабораторія Касперського.
  + Ліцензія (спосіб розповсюдження) - Власницьке програмне забезпечення.
  + Технічні характеристики програмного засобу та мінімальні вимоги до програмноапаратних засобів - Microsoft Windows, Linux.
  + Режим роботи виконання на базі клієнта.
  + Наявність Інтернет-підтримки – оновлення через інтернет.
  + Мова інтерфейсу - багатомовна.
  + Особливості управління об’єктами інтерфейсу програми - управління відбувається за допомогою миші та клавіатури, присутні гарячі клавіши, легкий у використанні.
  + Позитивні особливості програми.

1. Захист від вірусів, троянських програм і черв'яків є
2. Захист від шпигунських та рекламних програм
3. Перевірка файлів в автоматичному режимі і на вимогу
4. Перевірка поштових повідомлень (для будь-яких поштових клієнтів)
5. Перевірка інтернет-трафіку (для будь-яких інтернет-браузерів)
6. Захист інтернет-пейджерів (ICQ, MSN)
7. Проактивний захист від нових шкідливих програм
   * Можливі застосування програмного засобу.

Автоматичне налаштування програми в процесі установки. Готові рішення (для типових проблем). Наочне відображення результатів роботи програми