На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина 2

Одеса
19 квітня 2017 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 19 квітня 2017 р. - Одеса, Видавництво ОНАХТ, 2017 р. - 80 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови :

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., проф., директор НМАіР ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АВП ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІАтаМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ,
Сулімова Ю. – координатор IT–Cluster Odessa.

Члени оргокомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ,
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ,
Бойцова О.С. – заступник декана ФІТта КБ ОНАХТ,
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

Вкладка “Добавление абитуриента” содержит единую форму, на которой размещены поля для ввода информации об абитуриенте, необходимой в последующем. Большинство полей имеют флаг “required”, а также оснащены базовыми проверками. По итогу правильного заполнения формы создается сущность в базе данных, присваиваются номера личных дел в соответствии с выбранными специальностями.

Во вкладке “Список абитуриентов” находится таблица абитуриентов, содержащая минимальную информацию об абитуриентах. Здесь мы можем перейти на страницу просмотра, а также редактирования информации про абитуриента. Важно отметить, что любые действия по абитуриенту в системе будут сохранены и отображены в истории, будь то создание, редактирование или распечатка документов. Перейдя на страницу истории, мы можем видеть время каждого действия, кто его выполнил и его описание (при редактировании будет указано, какие именно поля были изменены, а также прошлое и текущее значение данного поля).

Также есть кнопка “Распечатать”, активирующая всплывающее окно со списком возможных для распечатки документов, таких как: заявления на каждую специальность, расписка в получении документов, бланк обработки данных абитуриента в Единой государственной электронной базе по вопросом образования.

Вкладка “Журналы абитуриентов” содержит список журналов на каждую специальность для дневной и заочной формы обучения. Журналы формируются согласно государственной формы. Фамилии абитуриентов сортируются по дате, при этом разбиваясь по разделам на каждый день.

В последующем планируется расширять функциональность, в первую очередь в сторону удобства абитуриентов. Возможно, будет добавлена онлайн подача заявления на вступление в учебное заведение, с регистрацией в очереди. Также в планах покрыть всю процедуру поступления - от подачи заявления до формирования рейтинга и распределения студентов по группам. Не могу не уделить внимания и внешнему виду приложения, в будущем планируется разработка специализированного дизайна. С увеличением сложности также будет уделяться внимание этапу тестирования и привлечению специалистов данной сферы.

ОГЛЯД І КЛАСИФІКАЦІЯ МЕРЕЖЕВИХ АТАК. МЕТОДИ БОРОТЬБИ

Шахов О.В. студент групи 531 факультета ІТ та КБ, ОНАХТЗ

Одним з головних завдань є забезпечення безпеки поводження інформації всередині мережі. Однією з небезпек для безпеки є мережеві атаки. Виникає два очевидних питання: «Які види мережевих атак бувають? Як їм протистояти? »

Мережеві атаки. Види. Способи боротьби

Мережева атака - дія, метою якого є захоплення контролю (підвищення прав) над віддаленою/локальної обчислювальної системою, або її дестабілізація, або відмова в обслуговуванні, а також отримання даних користувачів користуються цією віддаленої / локальної обчислювальної системою.

На даний момент виділяють наступні атаки: mailbombing, переповнення буфера, використання спеціалізованих програм (вірусів, сніфферов, троянських коней, поштових черв'яків, rootkit-ів і т.д.), мережева розвідка, IP-спуфинг, man-in-the-middle , ін'єкція (SQL-ін'єкція, PHP-ін'єкція, міжсайтовий скриптинг або XSS-атака, XPath-ін'єкція), відмова в обслуговуванні (DoS- і DDoS- атаки), phishing-атаки. Розглянемо кожну з них.

Mailbombing

Суть даної атаки полягає в тому, що на поштову скриньку надсилається величезна кількість листів на поштову скриньку користувача. Ця атака може викликати відмову роботи поштової скриньки або навіть цілого поштового сервера.

Переповнення буфера (buffer overflows)

Атака на переповнення буфера грунтується на пошуку програмних або системних вразливостей, здатних викликати порушення кордонів пам'яті та аварійно завершити додаток або виконати довільний бінарний код від імені користувача, під яким працювала вразлива програма. Якщо програма працює під обліковим записом адміністратора, то дана атака може дозволити отримати повний контроль над комп'ютером.

Використання спеціалізованих програм.

Робочі станції кінцевих користувачів дуже уразливі для вірусів і троянських коней. Вірусами називаються шкідливі програми, які впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача. Як приклад можна привести вірус, який прописується у файлі command.com (головному інтерпретаторі систем Windows) і стирає інші файли, а також заражає всі інші знайдені ним версії command.com.

«Троянський кінь» - це не програмна вставка, а справжня програма, яка виглядає як корисний додаток, а на ділі виконує шкідливу роль. Прикладом типового «троянського коня» є програма, яка виглядає, як проста гра для робочої станції користувача. Однак поки користувач грає в гру, програма відправляє свою копію електронною поштою кожному абоненту, занесеному в адресну книгу цього користувача. Всі абоненти отримують поштою гру, викликаючи її подальше поширення.

Сніффер пакетів є прикладною програмою, яка використовує мережеву карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому сниффер перехоплює всі мережеві пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і

аналізу трафіку. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніффер можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення імен і паролів створює велику небезпеку, так як користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і додатків. Якщо додаток працює в режимі клієнт / сервер, а аутентифікаційні дані передаються по мережі в читається текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів.

Rootkit - програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Більшість з реалізацій сучасних rootkit можуть ховати від користувача файли, папки і ключі реєстру, приховувати запущені програми, системні служби, драйвери і мережеві з'єднання. Тобто зловмисник має можливість створювати файли і ключі реєстру, запускати програми, працювати з мережею і ця активність не буде виявлена адміністратором. Крім того, rootkits можуть приховувати мережеву активність шляхом модифікації стека протоколів TCP/IP.

Мережева розвідка

Мережевий розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі зловмисник, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, луна-тестування (ping sweep) і сканування портів.

IP-спуфинг

IP-спуфинг відбувається, коли зловмисник, що знаходиться всередині корпорації або поза нею видає себе за санкціонованого користувача.

Атака типу man-in-the-middle

Для атаки типу Man-in-the-Middle зловмисникові потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера.

ОСОБЛИВОСТІ НАЛАШТУВАННЯ МАРШРУТИЗАТОРІВ МЕРЕЖІ ДОСТУПУ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ ПРОТОКОЛУ *ROUTING INFORMATION PROTOCOL*

Яворський Н.О., магістрант 553 гр., кафедра КІ, ОНАХТ, Одеса
керівник Бобрікова І.С., ст. викладач, кафедра КІ, ОНАХТ, Одеса

Анотація