

ДОДАТОК А
ПУБЛІКАЦІЯ ЗА ТЕМОЮ РОБОТИ

МАТЕРІАЛИ V МІЖНАРОДНОЇ
СТУДЕНТСЬКОЇ НАУКОВОЇ
КОНФЕРЕНЦІЇ

СУЧАСНІ АСПЕКТИ ТА
ПЕРСПЕКТИВНІ НАПРЯМКИ
РОЗВИТКУ НАУКИ



М. ХИТОМИР, УКРАЇНА

**9 ЧЕРВНЯ
2023 РІК**

СЕКЦІЯ 11.**ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ**

ЖИТТЄВИЙ ЦИКЛ СТАРТАПУ Домнішева А.П., Науковий керівник: Штих І.А.	132
КЕРУЮЧІ ПОВІДОМЛЕННЯ ПІДРІВНЯ МАС Виноградов М.М., Науковий керівник: Штих І.А.	134
КЛАСИФІКАЦІЯ АНТЕННИХ СИСТЕМ Мамедов Д.К., Науковий керівник: Штих І.А.	136
НАЛАШТУВАННЯ БЕЗПЕКИ МАРШРУТИЗАТОРІВ CISCO Житник В.Ю., Науковий керівник: Штих І.А.	138
ОСНОВНІ ПРАВИЛА ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ Чупахін Д.О., Науковий керівник: Штих І.А.	140
ПОБУДОВА ЗАХИЩЕНИХ МЕРЕЖ НА СЕАНСОВОМУ РІВНІ Москаленко Є.О., Науковий керівник: Штих І.А.	142
ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ ЛІКАРНІ Попадченко Г.А., Науковий керівник: Штих І.А.	144
ПРИХОВАНІСТЬ І ЗАВАДОЗАХИЩЕНІСТЬ У СИСТЕМІ ЗВ'ЯЗКУ WIMAX Гвінджілія К.А., Науковий керівник: Штих І.А.	146

СЕКЦІЯ 12.**КОМП'ЮТЕРНА ТА ПРОГРАМНА ІНЖЕНЕРІЯ**

АНАЛІЗ ПРОБЛЕМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДРОНІВ, ЩО ЗАСТОСОВУЮТЬСЯ У РОЗУМНИХ МІСТАХ Вечірська А.Д., Широкоград К.А., Науковий керівник: Вечірська І.Д.	148
ВИКОРИСТАННЯ GOOGLE APPS SCRIPT ДЛЯ РЕАЛІЗАЦІЇ DATA ACCESS LAYER У ПРОГРАМНИХ ЗАСОБАХ Гуренко Д.М., Науковий керівник: Іващенко Г.С.	150
ЗАСТОСУВАННЯ СИСТЕМ РОЗПІЗНАВАННЯ ЕМОЦІЙ ТА ПРОБЛЕМ ПОВ'ЯЗАНІ З ЇХ СТВОРЕННЯМ Кабанов О.Ф.	152
ПРОБЛЕМИ ГЕНЕРАЦІЇ ЗОБРАЖЕННЯ З ВИКОРИСТАННЯМ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ ТА СПОСОБИ ЇХ ВИРІШЕННЯ Кабанов О.Ф.	154
СУЧАСНІ МЕТОДИ ТА ЗАХОДИ ПРОВЕДЕННЯ ІТ-ОСВІТИ Кабанов О.Ф.	156
ФОРМАТ ОПИСУ КОМАНД ПРИ ОРГАНІЗАЦІЇ ВЗАЄМОДІЇ У ЗАСТОСУНКАХ ВІДДАЛЕНОГО ДОСТУПУ Зубенко Д.Р., Науковий керівник: Іващенко Г.С.	159

Житник Владислав Юрійович, здобувач вищої освіти
факультету інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Штих Інна Анатоліївна, старший викладач
кафедри радіотехнологій інформаційно-комунікаційних систем
Харківський національний університет радіоелектроніки, Україна

НАЛАШТУВАННЯ БЕЗПЕКИ МАРШРУТИЗАТОРІВ CISCO

На противагу звичній для нас життєвій мудрості: «Все, що не заборонено, - дозволено», з позицій захисту маршрутизатора будемо керуватися прямо протилежним постулатом: забороняти все, крім того, що дозволено. Крім цього, гарною ідеєю є заборона того функціоналу, який буде використовуватися рідко, не має сенсу у використанні або призначення якого нам не зовсім зрозуміле. Звісно, останній пункт має бути винятком, оскільки ми завжди можемо ознайомитися з величезним набором документації [1].

Загальний план фундаментального захисту маршрутизатора матиме такий вигляд [1]:

- налаштування аутентифікації та паролів;
- обмеження доступу до маршрутизатора;
- вимкнення зайвих служб і ввімкнення додаткових служб;
- налаштування SNMP;
- налаштування журналювання.

Підміна IP-АДРЕС – одна з критичних проблем протоколу IP версії 4, полягає вона в тому, що найчастіше більшість маршрутизаторів налаштовані на перенаправлення пакетів, виходячи тільки з даних у полі адреси призначення заголовка IP. Звісно, проблема полягає не в самому механізмі маршрутизації, а в тому, що в більшості мереж абсолютно будь-який коректно сформований пакет можна буде вільно перенаправити, якщо маршрутизатор матиме маршрут до адреси призначення, навіть якщо в полі адреси джерела заголовка IP буде вказано нелегітимну адресу. Подібна нелегітимна (фейк) адреса в умовах нормального функціонування мережі зазвичай не може бути вказана як джерело пакета, і найчастіше причиною її появи може стати лише те, що хтось, а точніше, щось не бажає показати, звідки насправді прийшов пакет [1].

Простіше кажучи, причиною появи в мережі подібних пакетів найчастіше є шкідливе програмне забезпечення, чи то хробаки, чи то віруси, чи то спам- або DDoS-боти. Звичайно, приховати їхню діяльність дуже складно, і будь-який більш-менш досвідчений мережний адміністратор за бажання досить швидко виявить їхню мережну активність. Візьмемо, наприклад, процес розсилки спаму. Найчастіше ним займатимуться керовані боти, особливий клас шкідливого програмного забезпечення на кшталт троянів-бекдорів, централізовано керованих із майстер-сервера. Спам-бот, коли отримав команду від господаря через майстер-сервер, у великій кількості розсилає кореспонденцію, відкриваючи безліч tcp-з'єднань на 25-ті порти (SMTP) різних серверів. При цьому в кеші маршрутизатора мережний

адміністратор спостерігає записи [1].

Як відомо, останнім часом атаки на кшталт TCP SYN-flood поступово сходять нанівець, завдяки старанням Microsoft щодо захисту своїх ОС Windows від неконтрольного використання сирих сокетів, що дають змогу конструювати мережні пакети "вручну". Зважаючи на вищезазвані обставини, дедалі більшої популярності набувають атаки на кшталт ICMP/UDP флуд або атаки, спрямовані на відмову в обслуговуванні Web-сервісів шляхом їхнього перевантаження POST/GET-запитами.

Список використаних джерел:

1. Уэнделл Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105: маршрутизация и коммутация, академическое издание. / акад. изд. : Пер. с англ. - М. : ООО. "И.Д. Вильямс", 2018. – 903 с.