УДК 681.3.06
DOI: 10.18372/2310-5461.36.12229

Б. Я. Корнієнко
д-р техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-2521-0878
e-mail: bogdanko@i.ua;

Л. П. Галата
Національний авіаційний університет
orcid.org/0000-0002-7978-3954
e-mail: galataliliya@gmail.com

ПОБУДОВА ТА ТЕСТУВАННЯ ІМІТАЦІЙНОГО ПОЛІГОНУ ЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вступ

Під час побудови імітаційного полігону захисту критичних інформаційних ресурсів, який складається з реального обладнання, виникає головна проблема, яку необхідно вирішити. Це висока вартість компонентів для побудови захищеної мережі. Для невеликих компаній побудова комп'ютерної мережі, задля тестування різних конфігурацій мережевого обладнання, гнучкого налаштування чи тестування різних політик безпеки на даному обладнанні є практично неможливою, оскільки для цього необхідні чималі фінансові витрати. Інколи, якщо компанія матиме все необхідне обладнання, то вона перш за все не буде надаватися для тестування тимчасової віртуальної мережі. Тому пропонується побудувати захищену комп'ютерну мережу на базі спеціальної платформи-емулятора, яка дозволяє віртуалізувати різне мережеве обладнання, створити на її базі повноцінну віртуальну мережу і виконати все необхідне тестування.

Мета статті

Проведення тестування побудованого імітаційного полігону захисту критичних інформаційних ресурсів.

Виклад основного матеріалу

Для побудови полігону імітаційного полігону захисту критичних інформаційних ресурсів на базі прикладного програмного забезпечення GNS3 обрано розповсюджену спрощену для невеликих підприємств топологію комп'ютерної мережі, з використанням одного брандмауера Cisco ASA 5520, який поділяє мережу компанії на демілітаризовану зону, внутрішню та зовнішню мережі [1–5]. Зональна модель є досить гнучкою, інтерфейси присвоюються зонам, а політика перевірки — трафіку, що передається між зонами (рис. 1).

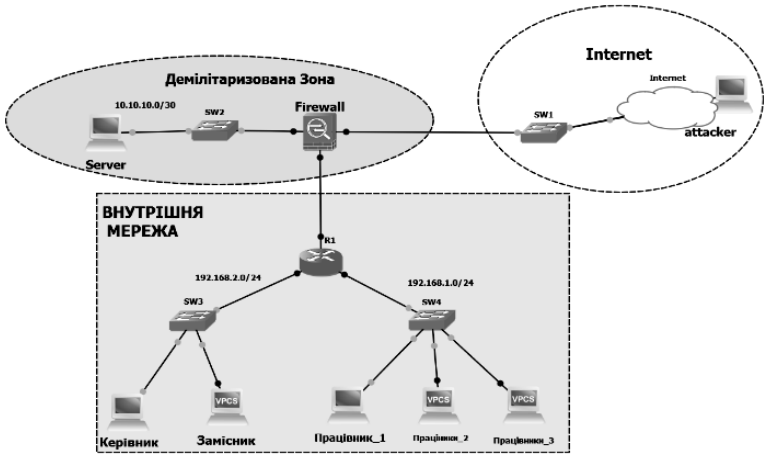

Рис. 1. Топологія мережі в GNS3

У даній топології для побудови імітаційного полігону захисту критичних інформаційних ресурсів використовують такі мережеві пристрої: міжмережевий екран Cisco ASA 5520 (ім'я хоста Firewall), маршрутизатор Cisco 3745 (ім'я хоста R1), мережеві комутатори (SW1, SW2, SW3,

SW4) [6–9]. Для надання доступу віртуальній мережі до Інтернету використовують loopback інтерфейс (Internet). Також у мережу додані дві віртуальні машини на операційній системі Windows 8.1 (Керівник-ПК, Працiв_1-ПК), аби імітувати реальні комп'ютери в мережі. Робочі станції працівників та замісника емулюються за допомогою VCPS тощо.

Мережа керівництва та мережа працівників знаходиться за інтерфейсом Gig1 міжмережевого екрану Firewall, за маршрутизацію трафіку між ними відповідає маршрутизатор R1 [10-11]. На Cisco ASA налаштовується NAT, для запобігання та обмеження запитів ззовні. Для більш зручних функцій керівництва і моніторингу налаштовується можливість підімкнення за протоколом HTTPS до ASDM. Доступ до Cisco ASDM здійснюється безпосередньо за допомогою Web-браузера з будь-якого комп'ютера мережі, що підтримує Java, таким чином, адміністраторам системи безпеки надається можливість швидкого і надійного доступу до пристроїв захисту Cisco ASA і має функціонал аналогічний консольному підключенню. Для безпечного віддаленого підімкнення до маршрутизатора R1 на ньому налаштовується SSH версії 2, а також заборонено всі інші з'єднання не по протоколу SSH. В демілітаризованій зоні знаходиться Server, який виконує функції Веб-сервера та FTP сервера. Веб-сервер доступний для керівництва та працівників, а також з мережі Інтернет. Користувачі мають доступ до Інтернету лише по 80-му порту та по ftp. Інші порти закриті. З мережі Інтернет доступ відкритий тільки на Веб-сайт і лише по 80-му порту.

Програмні засоби для тестування

Hping3 — це безкоштовний генератор пакетів і аналізатор для TCP/IP протоколу. Hping, де факто, один з обов'язкових інструментів для аудиту безпеки і тестування міжмережевих екранів і мереж, він використовувався для виконання експлойта техніки сканування Idle Scan, яка нині реалізована в сканері портів Nmap.

Як і більшість інструментів, що використовуються в комп'ютерній безпеці, hping3 корисний для експертів з безпеки та використовується для:

- traceroute/ping/probe (трасування/пінг/зондування) хостів;
- тестування правил брандмауера;
- тестування IDS (систем виявлення вторгнення);
- мережевих досліджень;
- стрес-тестувань мережі;
- вивчення TCP IP (hping була використана в мережевих курсах AFAIK);
- написання реальних програм, пов'язаних з TCP/IP тестуванням і безпекою;
- автоматизації тестів по фільтрації трафіку;
- створення робочої моделі експлойтів;
- досліджень у звірянні мереж і безпеки, коли потрібно емулювати комплексне TCP/IP поведінку.

Zenmap — офіційний GUI для програми Nmap Security Scanner. Zenmap — це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча добре впорається і з одиничними цілями. Zenmap використовує сирі IP-пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми і версію) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів/брандмауерів використовують і ще низку інших характеристик. У той час як Zenmap зазвичай використовується для перевірки безпеки, багатомережеві і системні адміністратори знаходять її корисною для звичайних завдань, таких як контролювання структури мережі, управління розкладами запуску служб і облік часу роботи хоста або служби.

Вихідні дані Nmap це список просканованих цілей з додатковою інформацією щодо кожної залежно від заданих опцій. Ключовий інформацією є «таблиця важливих портів». Ця таблиця містить номер порту, протокол, ім'я служби і стан. Стан може мати значення open (відкритий), filtered (фільтрується), closed (закритий) або unfiltered (не фільтрують). Відкрито означає, що додаток на цільовій машині готове для встановлення з'єднання/прийняття пакетів на цей порт. Фільтрування означає, що брандмауер, мережевий фільтр або якась інша перешкода в мережі блокує порт, і Nmap не може встановити відкритий цей порт або закритий. Закриті порти не пов'язані з жодним додатоком, так що вони можуть бути відкриті у будь-який момент [10].

Wireshark — це аналізатор мережевого трафіку. Його завдання полягає в тому, щоб перехоплювати мережевий трафік і відображати його в детальному вигляді. Wireshark може перехоплювати трафік різних мережевих пристроїв, відображая його ім'я (вмикая бездротові пристрої). Підтримування того або іншого пристрою залежить від багатьох факторів, наприклад від операційної системи та має безліч протокольних декодувальників (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS5, IMAP4, VNC, LDAP, NFS, SNMP, MSN, YMSG та ін.).

Wireshark дає змогу зберігати і відкривати раніше збережений мережевий трафік. Системні адміністратори використовують його для вирішення проблем в мережі, розробники використовують його для налагодження мережевих додатків, звичайні користувачі — для вивчення внутрішнього устрою мережевих протоколів.

Сканування мережі

Для сканування мережі обрано програму Zenmap — офіційний GUI (Graphical User Interface) для програми Nmap Security Scanner, утиліта для дослідження мережі та сканер портів. Для сканування обираються діапазони адрес для сканування задля економії часу. Проведено збирання інформації про мережу глобальної мережі, як наслідок налаштування NAT відображається лише налаштований інтерфейс Cisco ASA (рис. 2).

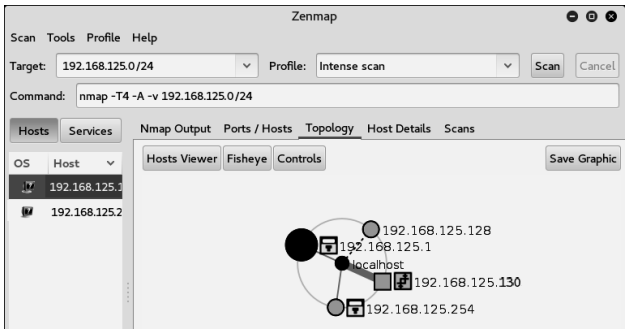

Рис. 2. Сканування локальної мережі з зовнішньої мережі

Якщо зловмисник має доступ до мережі зсередини, то йому вдасться просканувати топологію мережі і знайти можливі вразливості. Утиліта дозволяє визначити, які хости доступні в мережі (рис. 3), версію операційної системи, які служби на них запущені, назви запущених додатків і номера і стани портів. Якщо не заборонити стандартне підключення до маршрутизатора по мережевому протоколу Telnet, то Zenmap це виявить (рис. 4).

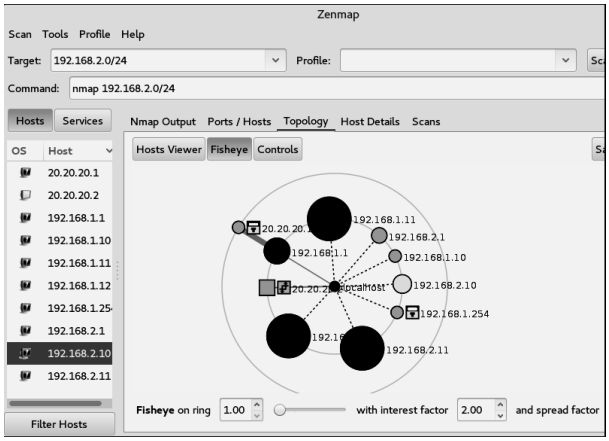

Рис. 3. Сканування локальної мережі зсередини

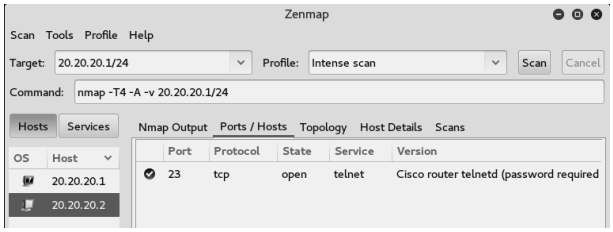

Рис. 4. Сканування маршрутизатора Cisco 3745 з увімкненим Telnet

У загальному вигляді після детального сканування мережевого пристрою матимемо результат утиліта Cisco 3745 з ввімкненим Telnet, утилітой Zenmap зроблено припущення щодо операційної системи, знайдено відкритий порт, визначена мережева адреса (рис. 5).

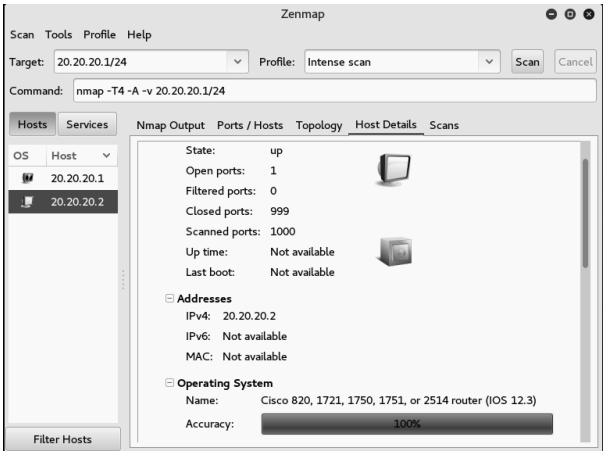

Рис. 5 Детальна інформація про відсканований Zenmap хост

На Cisco ASA присутній функціонал захисту від сканування, зокрема якщо в повідомленнях вказано одну і ту ж адресу джерела, це повідомлення може казати про збирання базових відомостей або спробу сканування портів та IP-пакет відхиляється ACL (рис. 6).

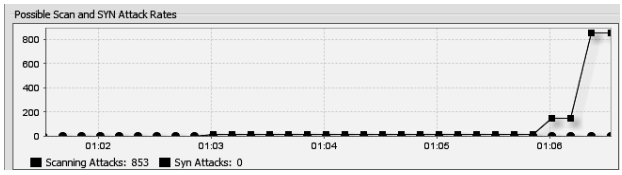

Рис. 6. Статистика відхилених пакетів Cisco ASA під час сканування мережі

Стрес-тест мереж

Атака на відмову в обслуговуванні (DoS) або атака на розподілену відмову в обслуговуванні (DDoS) — це спроба зробити ресурси машини недоступними для користувачів.

Хоча кошти, мотиви і цілі DoS розрізняються, головна її суть залишається незмінною — на час або на невизначений термін перервати або призупинити послуги хоста, з'єднаного з Інтернетом.

Один із загальних методів атаки — це насичення цільової машини зовнішніми запитами з'єднання, у зв'язку з чим вона не може відповісти на легітимний трафік або відповідає так повільно, що є по суті недоступною [11–12].

Syn-Flood Attack — це атака за якої ініціатор в пакеті SYN ставить підроблений Source IP-address або ігнорує відповіді від сервера Syn + Ack.

Під час відкриття тисячі таких половинчастих сесій витрачаються ресурси сервера, який змушений запам'ятовувати параметри кожної, і в підсумку може відмовити.

Для проведення DoS використаємо влаштовану в збірку Kali Linux утиліту hping3 використовуючи випадкові IP-адреси джерела DoS.

Дана програма без графічного інтерфейсу, для здійснення Syn-Flood Attack атаки обрані такі команди, як показано на рис. 7:

- hping3 — ім'я додатка;
- c 10000 — кількість пакетів для відправки;
- d 120 — розмір кожного пакету, який буде відправлений на цільову машину;
- S — відправка тільки пакети SYN;
- w 64 — розмір вікна TCP;
- p 80 — порт призначення, ви можете використовувати будь-який порт;
- flood — відправлення пакетів так швидко, як можливо, не піклуючись про відображення вхідних пакетів (Syn-Flood Attack);
- rand-source — використання випадкових IP-адрес джерела. Також можна використовувати -a або -spoof щоб заховати ім'я хоста;
- 192.168.125.130 — цільова IP-адреса або IP-адреса цільової машини. Також можна використовувати адресу сайту.

Cisco ASA автоматично транслює пакети, які надходять до неї по 80 порту на сервер, а при атаці на відмову ресурсів це спричиняє додаткового навантаження на сервер, що спричиняє відмову у доступі звичайним користувачам.

Пропінгуємо мережу без навантаження (результат показано на рис. 8) та мережу під навантаженням (рис. 9). А також скористаємось програмою Wireshark, за допомогою якої можна проаналізувати проведену DoS атаку. Відфільтрувавши прослуханий за допомогою Wireshark трафік між зловмисником та Cisco ASA за критерієм ICMP можна побачити, що в зв'язку з DoS атакою створюється навантаження на Cisco ASA, у зв'язку з яким створюються черги на оброблення запитів і відповіді приходять з певною затримкою або відповідь відсутня взагалі, як показано на рис. 10.

```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168
.125.130
HPING 192.168.125.130 (eth0 192.168.125.130): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Рис. 7. DoS-атака в hping3

```
C:\Users\EON>ping 192.168.125.130 -n 10

Обмен пакетами с 192.168.125.130 по с 32 байтами данных:
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=3мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=2мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=15мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=8мс TTL=255
Ответ от 192.168.125.130: число байт=32 время=1мс TTL=255

Статистика Ping для 192.168.125.130:
    Пакетов: отправлено = 10, получено = 10, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 15 мсек, Среднее = 3 мсек
```

Рис. 8. Пінг мережі без навантаження

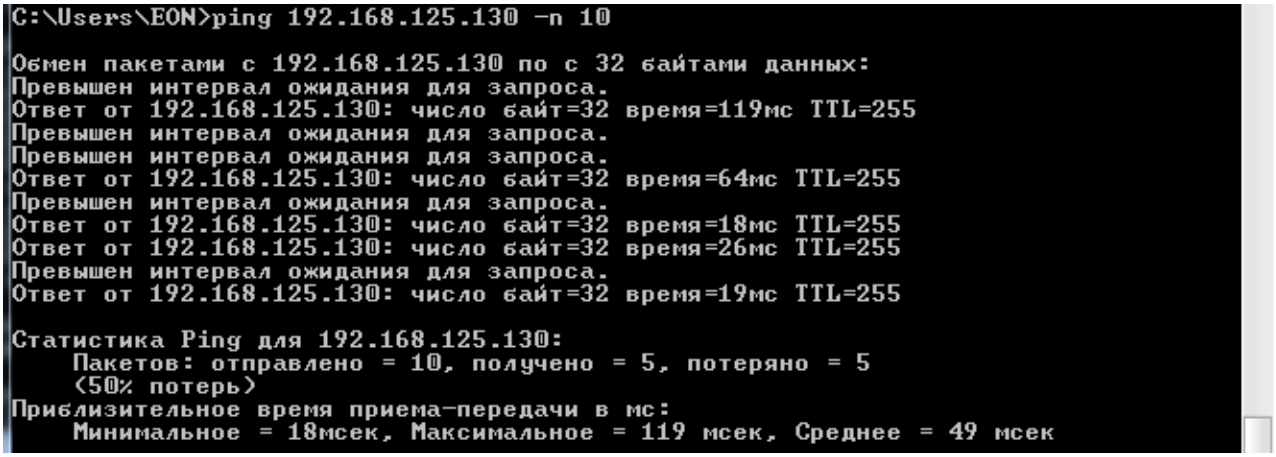

Рис. 9. Пінг-мережі під навантаженням 10 000 пакетів/секунду

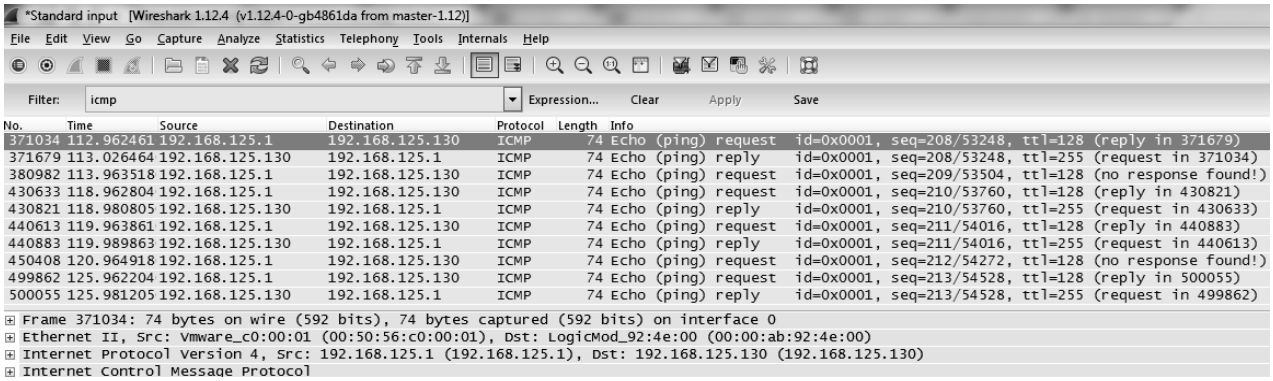

Рис. 10. Відфільтрований ICMP трафік під час DoS-атаки

Для вирішення даної проблеми ASA використовує TCP SYN Cookies:

ASA захищає сервер і не транслює на нього всі з'єднання.

Замість того, щоб запам'ятовувати всі ці половинчасті сесії, ASA відповідає на кожну з них, але фактичне з'єднання з сервером здійснює тільки при отриманні 3-ї відповіді Ack.

Embryonic-conn-max п'ять означає, що максимум буде дозвіл до п'яти половинчастих з'єднань. Необхідно задати такі налаштування:

– access-list outside_mpc line 1 extended permit tcp any object dmz-server real;
– class-map no-syn-flood-class;
– match access-list outside_mpc;
– policy-map NO-SYN-FLOOD;
– class no-syn-flood-class;
– set connection conn-max 0 embryonic-conn-max 5 per-client-max 0 per-client-embryonic-conn-max 0 random-sequence-number enable;
– service-policy NO-SYN-FLOOD interface outside.

Без додаткових налаштувань, при Syn-Flood атаці, відбувається 1625 активних підключень до сервера, що й спричиняє відмову в обслуговуванні.

Якщо застосувати дані налаштування ASA, буде створювана окрема черга з половинчастих сесій, які не зможуть кардинально вплинути на роботу сервера, як наслідок отримаємо лишень п'ять половинчастих з'єднань, що свідчить про ефективність захисту відданого типу атак при правильному налаштування міжмережевого екрану.

Висновки

Таким чином, для випробовування побудованого полігону кібербезпеки було розглянуто програмні засоби для проведення тестування побудованого полігону кіберпезбеки та проведено сканування мережі та портів мережевих пристроїв за допомогою утиліти Zenmap ззовні.

Як наслідок налаштувань ASA та NAT, сканування не дало нічого окрім знайденої IP-адреси зовнішнього інтерфейсу ASA, та сканування зсередини, у результаті якого була зібрана інформація про внутрішню мережу включаючи внутрішній інтерфейс Cisco ASA.

За допомогою утиліти hping3 було реалізовано стрес-тест мережі — Syn-Flood атака на відмову сервера. Реалізовано протидію даній атаці щляхом використання TCP SYN Cookies.

ЛІТЕРАТУРА

1. **Сергієнко І. В.** Інформатика в Україні: Становлення, розвиток, проблеми / І. В. Сергієнко. — К. : Наук. думка, 1999. — 354 с.

2. **Korniyenko B. Y.** Design and research of mathematical model for information security system in computer network / B. Y. Korniyenko, L. P. Galata // Наукоємні технології. — 2017, № 2 (34). — С. 114–118.

3. **Корнієнко Б. Я.** Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки / Б. Я. Корнієнко // Наукоємні технології. — 2012, № 3 (15). — С. 83–89, doi.org/10.18372/2310-5461.15.5120 (ukr).

4. **Korniyenko B. Y.** Open systems interconnection model investigation from the viewpoint of information security / B. Korniyenko, O. Yudin, E. Novizkij // The Advanced Science Journal. — 2013. — Issue 8. — P. 53–56.

5. **Корнієнко Б. Я.** Реалізація інформаційної безпеки у моделі взаємодії відкритих систем / Б. Я. Корнієнко, О. К. Юдін / Збірник тез VI Міжнародної науково-технічної конференції «Комп'ютерні системи та мережні технології» (CSNT-2013), 11–13 червня 2013 р. — С. 73.

6. **Корниенко Б. Я.** Информационная безопасность и технологии компьютерных сетей: монография / Б. Я. Корниенко // ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. — 2016. — 102 с.

7. **Korniyenko B.** Modeling of security and risk assessment in information and communication system / Korniyenko B., Galata L., Kozuberda O. / Sciences of Europe. — 2016. — V. 2. — No 2 (2). — P. 61–63.

8. **Korniyenko B.** The classification of information technologies and control systems / B. Korniyenko // International scientific journal. — 2016. — № 2. — P. 78–81.

9. **Korniyenko B.** Risk estimation of information system / B. Korniyenko, A. Yudin, L. Galata // Wschodnioeuropejskie Czasopismo Naukowe. — 2016. — № 5. — P. 35–40.

10. **Корнієнко Б. Я.** Безпека аутентифікації у Web-ресурсах / Б. Я. Корнієнко, О. К. Юдін, О. С. Снігур / Науково-практичний журнал «Захист інформації». — 2012. — № 1 (54). — С. 20–25, doi.org/10.18372/2410-7840.14.2056 (ukr).

11. **Корнієнко Б. Я.** Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська / Науково-практичний журнал «Захист інформації», 2012. — № 4 (57). — С. 60–64, doi.org/10.18372/2410-7840.14.3493 (ukr).

12. **Корниенко Б. Я.** Кибернетическая безопасность — операционные системы и протоколы / Б. Я. Корниенко // ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2017. — 122 с.

Корнієнко Б. Я., Галата Л. П.

ПОБУДОВА ТА ТЕСТУВАННЯ ІМІТАЦІЙНОГО ПОЛІГОНУ ЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті розглянуто процес побудови імітаційного полігону як способу вивчення поведінки системи захисту критичних інформаційних ресурсів. Для побудови імітаційного полігону використовується прикладна програма Graphical Network Simulator. Досліджено функціональні можливості пакету GNS3. Розглянуто основні властивості імітаційного полігону захисту критичних інформаційних ресурсів. Здійснено тестування побудованого імітаційнийного полігону захисту критичних інформаційних ресурсів програмними засобами та проведено сканування мережі та портів мережних пристроїв за допомогою утиліти Zenmap. Зібрана інформація про внутрішню мережу та внутрішній інтерфейс Cisco ASA. За допомогою утиліти hping3 реалізовано стрес-тест мережі — Syn-Flood атака на відмову сервера. Реалізовано протидію даній атаці шляхом використанням TCP SYN Cookies.

Ключові слова: імітаційний полігон, критичні інформаційні ресурси, безпека, загрози, тестування.

Корниенко Б. Я., Галата Л. П.

ПОСТРОЕНИЕ И ТЕСТИРОВАНИЕ ИМИТАЦИОННОГО ПОЛИГОНА ЗАЩИТЫ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В данной статье рассмотрен процесс построения имитационного полигона как способа изучения поведения системы защиты критических информационных ресурсов. Для построения имитационного полигона используется приложение Graphical Network Simulator. Исследованы функциональные возможности пакета GNS3. Рассмотрены основные свойства имитационного полигона защиты критических информационных ресурсов. Осуществлено тестирование построенного имитационного полигона защиты критических информационных ресурсов программными средствами и проведено сканирование сети и портов сетевых устройств с помощью утилиты Zenmap. Собрана информация о внутренней сети и внутреннем интерфейсе Cisco ASA. С помощью утилиты hping3 реализовано стресс-тест сети — Syn-Flood атака на отказ сервера. Реализовано противодействие данной атаке путем использования TCP SYN Cookies

Ключевые слова: имитационный полигон, критические информационные ресурсы, безопасность, угрозы, тестирование.

Korniyenko B. Y., Galata L. P.

CONSTRUCTION AND TESTING OF THE SIMULATION POLYGON FOR THE PROTECTION OF CRITICAL INFORMATION RESOURCES

In this article, the process of constructing an imitation polygon as a method for studying the behavior of the system of protection of critical information resources is considered. The graphical network simulator application is used to construct the simulation polygon. The functionality of the GNS3 package is explored. The main properties of the simulation ground of protection of critical information resources are considered. The testing of a built-up simulation ground for protecting critical information resources by software was performed and network port scan was performed using the Zenmap utility. Information on the internal network and internal interface of Cisco ASA are gathered. Using the hping3 utility, a stress test of the network is implemented - the Syn-Flood attack on the server's failure. The counteraction of this attack with the use of TCP SYN Cookies is implemented.

Keywords: simulation polygon, critical information resources, security, threats, testing.

Стаття надійшла до редакції 28.11.2017 р.
Прийнято до друку 29.11.2017 р.
Рецензент — д-р техн. наук, проф. Щербак Л. М.