ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.53

Защита SSH-порта с использованием имитации уязвимостей Honeypot

Д.О. Дедов
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Российская Федерация

Аннотация. Представлено исследование, направленное на анализ безопасности компьютерных сетей с использованием комплексного подхода, который включает в себя экспериментальную среду с двумя ПК, на которых установлена операционная система Kali Linux, и инструментарий Pentbox. Целью работы являлось повышение эффективности системы Honeypot в сфере обеспечения безопасности сети. Создан экспериментальный стенд, состоящий из двух компьютеров — атакующего и защищающегося. Проведен подробный анализ системы Honeypot, включая эмуляцию различных сетевых протоколов, таких как TCP, HTTP и DNS. Кроме того, в ходе исследования проведена атака на SSH-сервер с использованием инструмента Hydra для брутфорс-атаки. Эмуляция уязвимостей может быть полезна как для организаций, так и для специалистов в области информационной безопасности, помогая им принять соответствующие меры по защите своих компьютерных сетей.

Ключевые слова: кибербезопасность, пентест, приманка, брутфорс-атака, эмуляция уязвимостей

Securing an SSH Port Using Honeypot Vulnerability Simulation

Danil O. Dedov
St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russian Federation

Abstract. The paper presents a study aimed at analyzing the security of computer networks using an integrated approach, which includes an experimental environment with two PCs running the Kali Linux operating system and the Pentbox toolkit. The aim of the work was to increase the efficiency of the Honeypot system in the field of network security. An experimental stand has been created, consisting of two computers — an attacker and a defender. A detailed analysis of the Honeypot system has been carried out, including emulation of various network protocols such as TCP, HTTP and DNS. In addition, during the study, an attack was carried out on an SSH server using the Hydra tool for a brute force attack. Vulnerability emulation can be useful for both organizations and information security professionals, helping them take appropriate measures to protect their computer networks.

Keywords: cybersecurity, pentest, honeypot, bruteforce attack, vulnerability emulation

Введение. В наше время при растущем влиянии Интернета и увеличении числа цифровых атак киберпреступники проявляют все большую изобретательность. За последний год в России отмечено заметное увеличение компьютерных атак, особенно в контексте геополитических напряжений. Это приводит к активным хакерским атакам на веб-ресурсы российских компаний и организаций [1]. В современной литературе замечается дефицит исследований, посвященных эффективным методам противодействия киберугрозам. Несмотря на наличие технологии Honeypot для обнаружения, анализа и сбора информации о киберугрозах [2, 3], особое внимание уделяется недостаточной кибербезопасности, в частности, не защищенному SSH-порту, который представляет собой ключевую уязвимую точку для злоумышленников [4]. В предлагаемом подходе используется приманка с уязвимостями — Honeypot для защиты SSH-порта. Это исследование вносит существенный вклад в научные знания об информационной безопасности [5].

Основная цель данного исследования заключалась в разработке эффективного подхода к повышению кибербезопасности сети и SSH-порта с использованием технологии Honeypot. В рамках поставленных целей проведен анализ известных и неизвестных существующих угроз в контексте SSH-порта, а также определены оптимальные методы их выявления и предотвращения. Помимо этого, проведена оценка эффективности предложенного подхода и выявлены, в сравнении с существующими методами, его преимущества [6].

Основная часть. Для организации стенда использовалась утилита Pentbox. Pentbox — эффективный инструмент безопасности, используемый для пентенста, создающий разные типы Honeypot (рис. 1) [7].

Рис. 1. Интерфейс утилиты Pentbox

SSH Honeypot имитирует уязвимость в SSH-сервере и фиксирует действия злоумышленников, пытающихся воспользоваться этой уязвимостью. Web Honeypot, в свою очередь, имитирует уязвимость в веб-сервере, ловлю злоумышленников и отслеживание их действий. A DNS Honeypot выявляет уязвимость в DNS-сервере, предоставляя возможность отслеживать действия злоумышленников, стремящихся использовать данную уязвимость. Pentbox также позволяет настраивать различные параметры приманки, включая IP-адрес, порт и настройки логирования. Простой и удобный интерфейс управления Honeypot делает этот инструмент доступным для широкого круга пользователей. Все настройки можно легко изменить через интерактивный командный интерфейс [8].

В контексте структуры сети приманка размещается на узлах между коммутатором и роутером, а также перед брандмауэром, защищающим локальную сеть предприятия (рис. 2). Это стратегическое распределение позволяет эффективно обнаруживать и отслеживать потенциальные атаки, направленные на систему [9, 10].

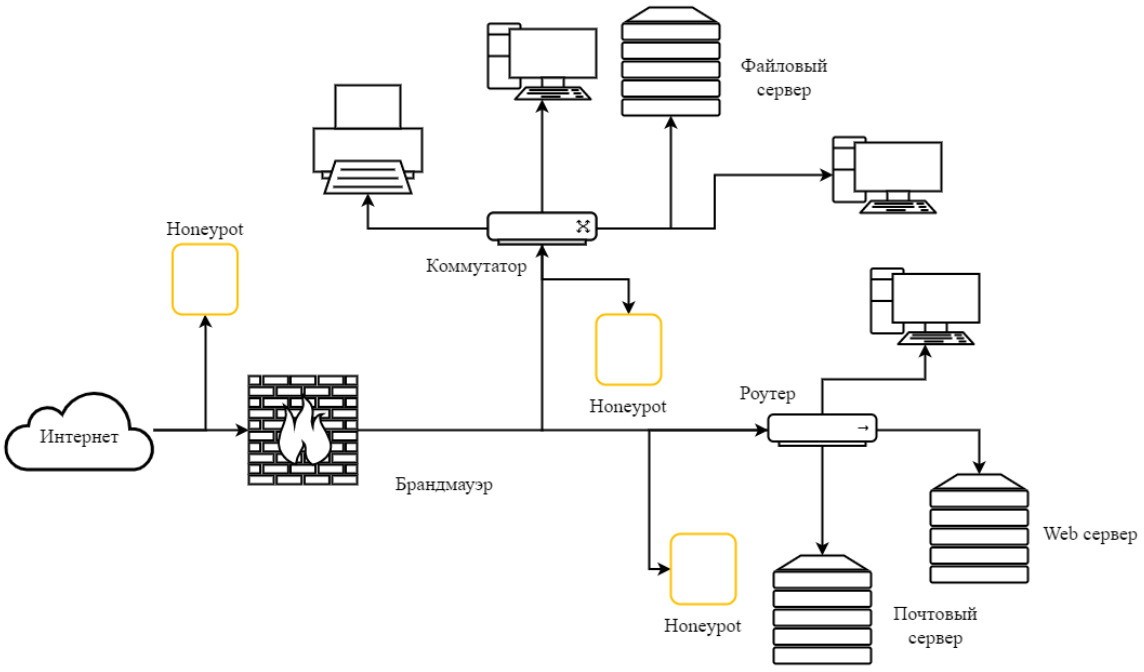

Рис. 2. Схема установки Honeypot в организациях

Для демонстрации функциональности Pentbox и его возможностей выбрана атака Bruteforce SSH. Опираясь на анализ графических данных от Positive Technologies, можно сделать вывод, что атаки подбора паролей, то есть Bruteforce, находятся в списке наиболее популярных атак. (рис. 3). Основная цель проведения Bruteforce SSH — показать способность утилиты выявлять и предотвращать подобные атаки [11].

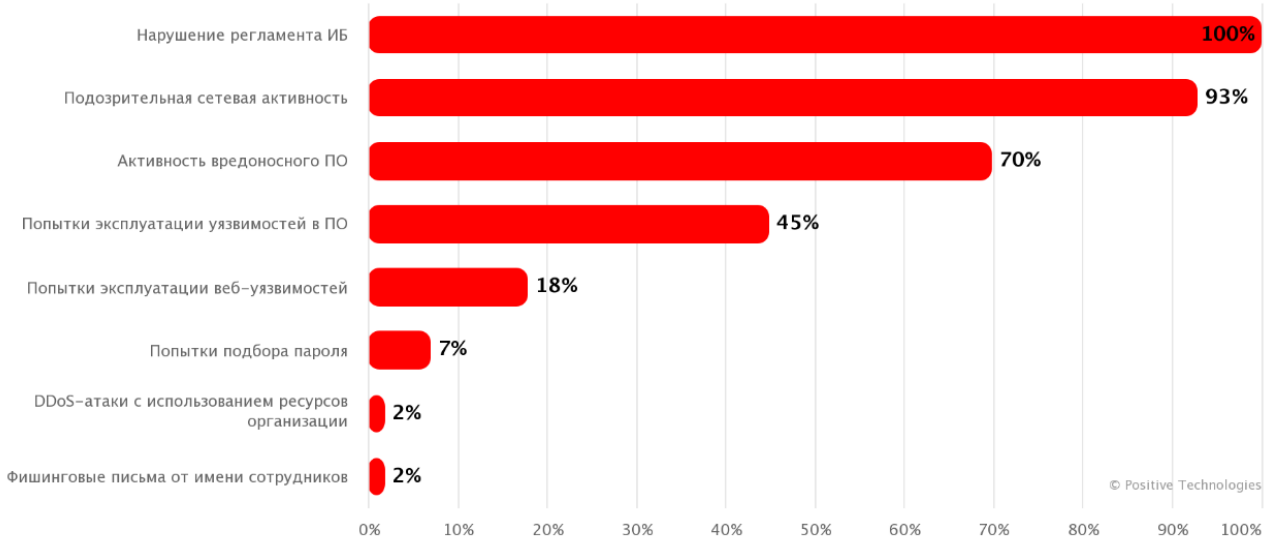

Рис. 3. Категории выявленных компанией Positive Technologies угроз

Для демонстрации атаки в программе-имитаторе GNS3, предназначенной для моделирования компьютерных сетей, был создан макет [12]. Этот инструмент позволяет виртуально моделировать сетевые структуры с различными устройствами, такими как маршрутизаторы, коммутаторы и межсетевые экраны. Макет включает два узла Kali Linux: один выступает в роли атакующего, другой — в роли защищающегося [13]. Для создания реалистичной сетевой среды использовали коммутаторы (рис. 4), проектируя сеть в программе GNS3. Выбор пал на Kali Linux из-за его множества инструментов, таких как сканеры уязвимости, средства проведения атак, анализаторы сетевого трафика и приложения для анализа безопасности беспроводных сетей. Операционная система Kali Linux также поддерживает различные методы атак, включая социальную инженерию, фишинг, взлом паролей и использование эксплойтов [14]. В анализируемой сети для обеспечения ее функционирования используются коммутаторы Ethernet и маршрутизатор Cisco.

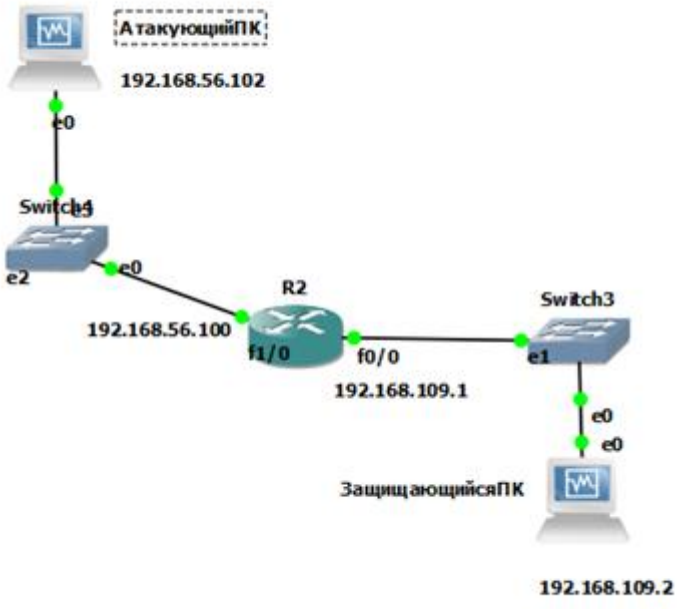

Рис. 4. Схема стенда для моделирования атаки Bruteforce
(схема спроектирована в программе GNS3)

На защищаемом компьютере была запущена утилита Pentbox, эмулирующая открытие портов серверов и служб. Атакующий, собрав данные, успешно провел разведку сети (рис. 5) [15]. Результаты указывают на наличие открытого порта 22, обычно используемого сервером SSH. Этот открытый порт является виртуальной реализацией функциональности сервера SSH, эмулируемой Pentbox. Атакующий использовал для разведки сети программу Nmap — инструмент анализа сети с открытым исходным кодом. Nmap позволяет выявлять активные устройства, доступные порты, определять операционные системы и предоставлять возможности для анализа безопасности сети, аудита системы и выявления уязвимостей. Программа выявляет наличие открытого порта 22, который незаметно сливается с обычным портом в сети.

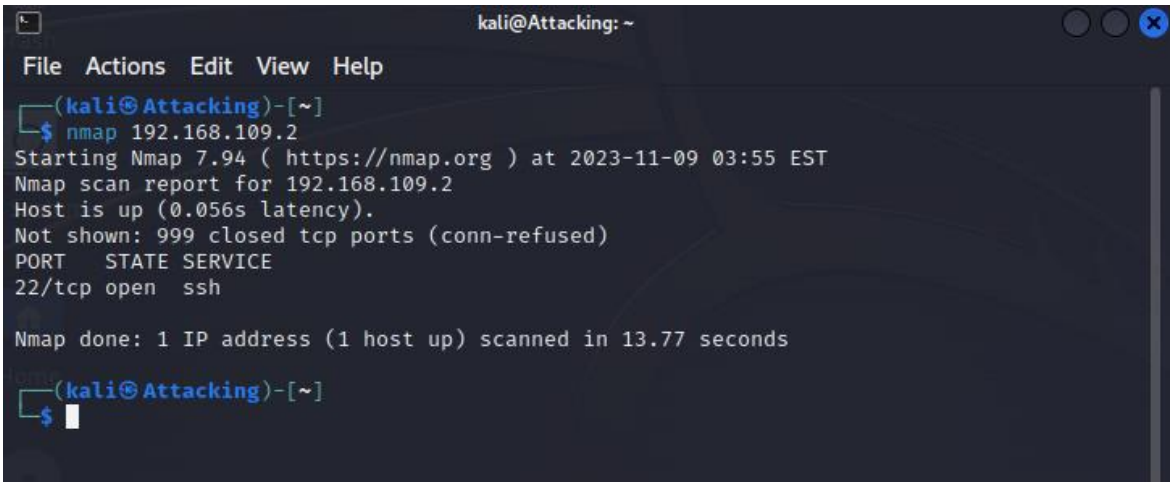

Рис. 5. Проведение сканирования атакующим ПК

Атакующий компьютер проводит Bruteforce — атаку, которая осуществляется командой с заранее заданными опциями на указанный порт с использованием Hydra. Завершив атаку, защищающийся компьютер регистрирует информацию об инциденте. Данные об инциденте детально описаны в отчете о состоянии порта (рис. 6).

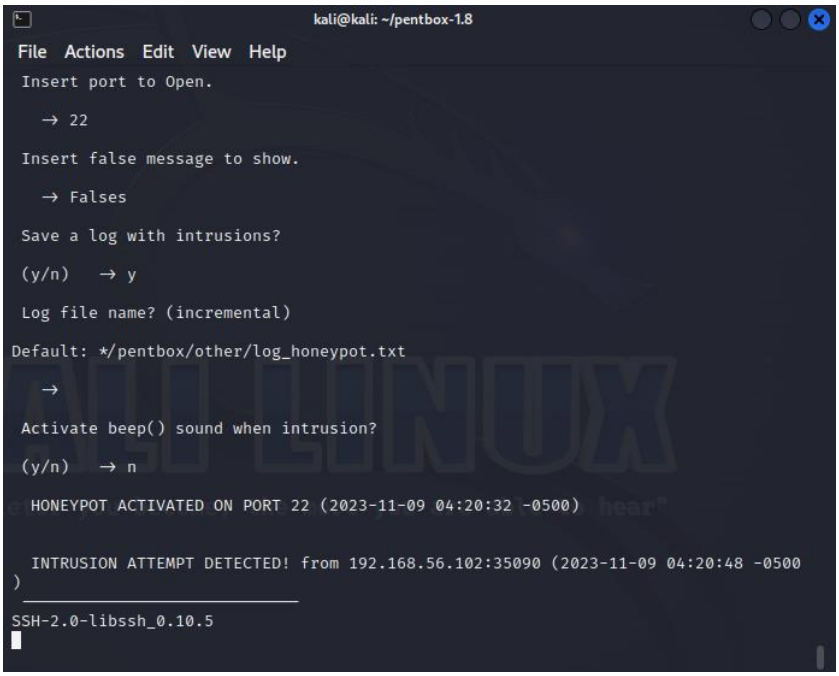

Рис. 6. Уведомление honeypot об обнаружении атаки

Pentbox автоматически регистрирует данные об атаках, а приманка защищает порт SSH от несанкционированного доступа. Эксперименты подтверждают высокую эффективность этого подхода при выявлении и блокировке атак методом перебора паролей (Bruteforce).

Заключение. В рамках исследования успешно подтверждена эффективность программы Pentbox в обнаружении и защите от атак типа Bruteforce. Проведенные эксперименты, в том числе контрольная атака и использование утилиты, привели к достижению необходимых результатов, позволяя оценить ее производительность. Pentbox проявила выдающуюся эффективность при мониторинге сетевой активности, предоставляя ценную информацию о затронутых запросах. Ее функционал по отслеживанию и реагированию на подозрительную сетевую активность способствует предотвращению потенциальных угроз и повышению кибербезопасности.

Для организаций и сетевых администраторов Pentbox является ценным инструментом, способным эффективно противостоять распределенным атакам и минимизировать риски для информационной инфраструктуры. Его практическое значение заключается не только в обеспечении надежной защиты сети, предоставлении важной информации для анализа и принятия решений, но и в снижении негативных последствий от атак. Эффективность стратегического внедрения Pentbox может быть дополнительно усилена взаимодействием с другими средствами защиты системы. Например, совместное использование с межсетевыми экранами, системами обнаружения вторжений (IDS) и системами предотвращения вторжений (IPS) расширяет спектр защиты от различных видов атак [16].

Важно отметить, что несмотря на мощь Pentbox в выявлении и защите от Bruteforce, его эффективность может быть дополнительно увеличена при совместном использовании с другими средствами системной безопасности.

Список литературы

1. Kumar S. Hacking attacks, methods, techniques and their protection measures. *International Journal of Advance Research in Computer Science and Management*. 2018;4(4):2253–2257.

2. Umamaheswari A., Kalaavathi B. Honeypot TB-IDS: trace back model based intrusion detection system using knowledge based honeypot construction model. *Cluster Computing*. 2019;22(6):14027–14034. https://doi.org/10.1007/s10586-018-2173-4

3. Kuwatly I., Sraj M., Masri Z. Al., Artail H. A dynamic honeypot design for intrusion detection. In: ACS *International Conference on Pervasive Services, ICPS 2004.* Proceedings. Beirut, Lebanon: IEEE; 2004. P. 95–104. https://doi.org/10.1109/PERSER.2004.1356776

4. Veena K., Meena K. Implementing file and real time based intrusion detections in secure direct method using advanced honeypot. *Cluster Computing*. 2019;22(6):13361–13368. https://doi.org/10.1007/s10586-018-1912-x

5. Авдошин А.С., Шатунов П.П. Применение honeypot-ловушек для сбора данных о кибератаках на промышленные сети. *Известия Волгоградского государственного технического университета. Серия: Новые образовательные системы и технологии обучения в вузе*. 2010;7(8):16–18.

6. Owens J., Matthews J.N. A study of passwords and methods used in brute-force SSH attacks. *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*. 2008.

7. How to install Honeypot on Kali Linux. URL: https://buffercode.in/how-to-install-honeypot-on-kali-linux/ (дата обращения: 09.11.2023).

8. Ping Wang, D'Cruze H. Honeypots and knowledge for network defense. *Issues in Information Systems*. 2021;22(3):241–254. https://doi.org/10.48009/3_iis_2021_259-272

9. Кулябов Д.С., Ульянов А.В. О целях и задачах проекта Honeynet. *Вестник Российского университета дружбы народов. Серия: Прикладная и компьютерная математика.* 2004;3(1)162–178.

10. Максин И. С. Выявление подозрительной активности в распределенных информационных сетях с использованием перспективной технологии сетей приманок (HONEYNET). *Информационная среда образования и науки*. 2013;(17):42–46.

11. Positive Technologies. *Обнаружение распространенных угроз ИБ в сетевом трафике*. URL: https://www.ptsecurity.com (дата обращения: 09.11.2023).

12. Dayananda Lal N., Behnam Ghorbani, Solmaz Vaghri. A survey on the use of GNS3 for virtualizing computer networks. *International Journal of Computer Science and Engineering.* 2016;5(1):49–58. URL: https://www.semanticscholar.org/paper/A-SURVEY-ON-THE-USE-OF-GNS3-FOR-VIRTUALIZING-lal-Ghorbani/687de1f90b0c70a6303c8ab8067869becf97dd77 (дата обращения: 09.11.2023).

13. Emiliano R., Antunes M. Automatic network configuration in virtualized environment using GNS3. In: *10th International Conference on Computer Science & Education (ICCSE)*. Cambridge, UK; 2015. P. 25–30. https://doi.org/10.1109/ICCSE.2015.7250212

14. Sultan Al-Jameel, Adwan Alownie Alanazi. Honeypots tools study and analysis. *International Journal of Computer Science & Network Security*. 2021;21(1):162–173. https://doi.org/10.22937/IJCSNS.2021.21.1.21

15. Miller B.P., Cui-Qing Yang. IPS: An interactive and automatic performance measurement tool for parallel and distributed programs. In: *Proc. of the Seventh Conference on Distributed Memory Computer Systems.* 1987. P. 482–489.

16. Baier P., Pennerstorfer J., Schopf A. PHENIPS—a comprehensive phenology model of Ips typographus (L.)(Col., Scolytinae) as a tool for hazard rating of bark beetle infestation. *Forest Ecology and Management*. 2007;249(3):171–186. https://doi.org/10.1016/j.foreco.2007.05.020

Об авторах:

Дедов Данил Олегович, студент кафедры информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения, (190121, РФ, г. Санкт-Петербург, Большая Морская улица, 67), Dedovdanil3@yandex.ru

About the Author:

Danil O. Dedov, Student of the Information Security Department, Saint Petersburg State University of Aerospace Instrumentation (67, Bolshaya Morskaia St., Saint Petersburg, 190121, RF), Dedovdanil3@yandex.ru