УДК 004.056.53

ИНФОРМАЦИОННАЯ СИСТЕМА ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

Лызо Д.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Радненок А.Л. – магистр техн. наук, ст. преподаватель

Аннотация. В настоящее время, благодаря процессам информатизации и использования сети Интернет люди получают возможность осуществлять не только коммуникации, но и совершать платежи, работать, использовать развлекательные ресурсы и многое другое. Количество активных пользователей сети за последние несколько лет динамично увеличивается, и прирост каждый год составляет более 100 миллионов человек. Несмотря на большое количество разработанных средств, в частности, антивирусов, файерволов, брандмауэров, риск утечки информации весьма велик, и его необходимо снижать.

Ключевые слова. Безопасность, тестирование, атака, порт, сеть, проникновение.

Введение. Необходимо усовершенствование существующих систем информационной безопасности, расширение возможностей этих систем и объединение различных утилит в одну единую, с целью оптимизации проверки уязвимостей, которыми могут воспользоваться люди со злым умыслом.

Основная часть. Для тестирования безопасности компьютерной сети необходимо несколько этапов, схематически изображенных на рисунке 1.

Рисунок 1 – Этапы тестирования безопасности корпоративных сетей

Анализ проблем безопасности корпоративных сетей. Для анализа проблем безопасности корпоративных сетей необходимо изначально выяснить, для чего эти сети применяются. Затем происходит анализ крупных и средних инцидентов, произошедших за последние несколько лет, с целью актуализации известных общих проблем, а также как компании от них защищаются в данный момент.

Анализ известных методик тестирования и разработка частной методики. Данный шаг необходим для сравнения с текущими методиками тестирования безопасности компьютерной сети. Для решения этой задачи рассматривались существующие методики. Произведен анализ, который выявил, что эти методики не подходят по ряду причин, поэтому разработана частная методика тестирования, которая включает в себя некоторые моменты из уже существующих методик.

Разработка векторов атак. Используя схему сети компании N, создаются вектора атак, которые возможно использовать для тестирования на проникновение сети.

Тестирование на проникновение с учетом полученных данных на предыдущих шагах, оценка степени критичности выявленных уязвимостей с учетом выработанных ранее векторов атак, а также разработка рекомендаций по устранению этих уязвимостей и оценка уровня защищенности.

Для этого шага произведено тестирование на проникновение в сервисы сети компании N. Проанализированы полученные данные и оценен возможный риск.

Информационная система представляет собой набор утилит, разработанных с помощью языка программирования *Python (WIG, WPScan, NSLookup)*, с использованием библиотек *Scapy / dpkt + pcapy, Impacket, Python Nmap, Requests / BeautifulSoup*. Для корректной работы всех используемых библиотек необходима операционная система для пенетрационного тестирования *Kali Linux*. Пример работы утилиты *WIG* представлен на рисунке 2.

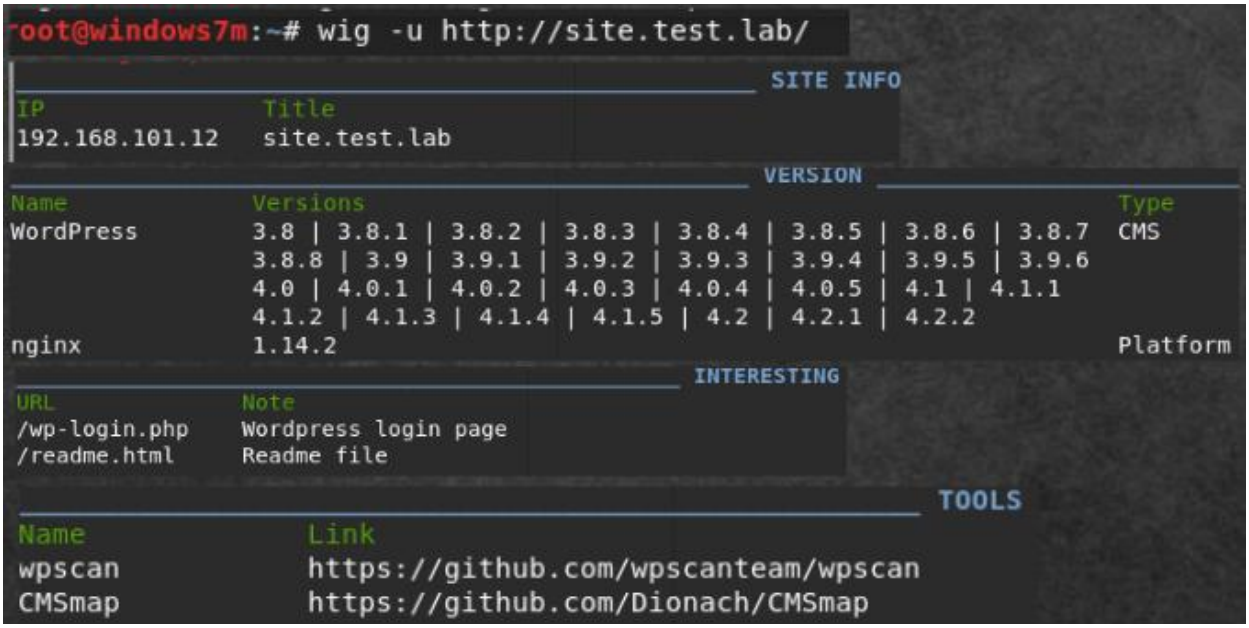

Рисунок 2 – Окно работы утилиты *WIG*

Пример работы утилиты Nmap представлен на рисунке 3.

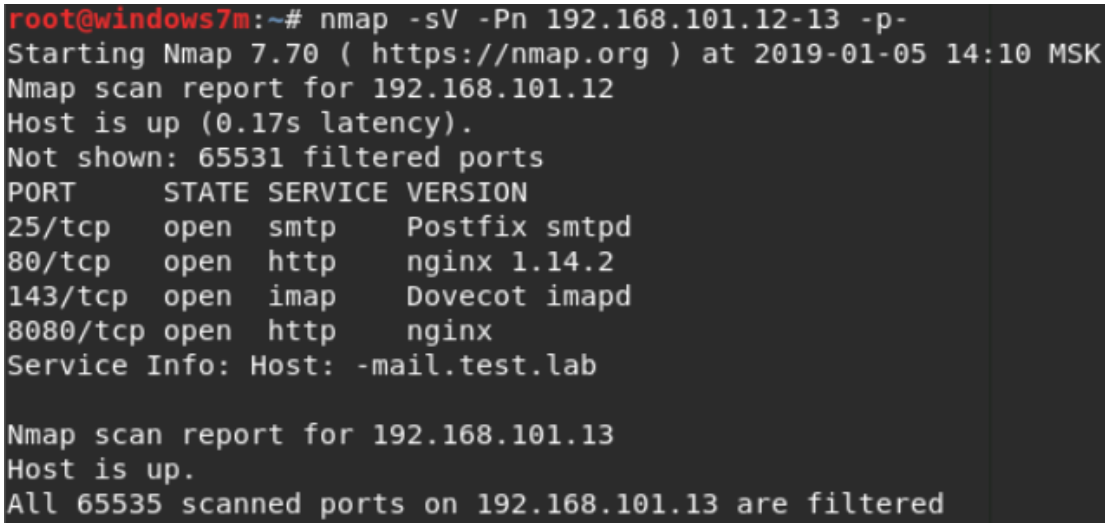

Рисунок 3 – Окно работы утилиты *Nmap*

Заключение. Результатом работы системы является выявления перечня возможных уязвимостей в сети компании N. Рекомендации по профилактике и пресечению конкретных проблем безопасности выдает специалист на основе полученных данных.

Список литературы

1. *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50 1st Edition, Kimberly Graves*
2. *BackTrack 5 Wireless Penetration Testing Beginner's Guide, Vivek Ramachandran*
3. *Black Hat Python: Python Programming for Hackers and Pentesters 1st Edition, Justin Seitz*

UDC 004.056.53

INFORMATION SYSTEM FOR TESTING THE SECURITY OF THE COMPUTER NETWORK

Lyzo D.P.

Belarusian State University of Informatics and Radioelectronics Minsk, Republic of Belarus

Radnenok A.L. - Master of Engineering Science, Senior Lecturer

Annotation. Currently, thanks to the processes of informatization and the use of the Internet, people are able to carry out not only communications, but also make payments, work, use entertainment resources and much more. The number of active Internet users has been dynamically increasing over the past few years, and the growth is over 100 million people every year. Despite the large number of developed tools, in particular, antiviruses, firewalls, firewalls, the risk of information leakage is very high, and it must be reduced. For this purpose, it is necessary to improve existing information security systems, expand the capabilities of these systems and combine various utilities into one single one, in order to optimize the verification of vulnerabilities that can be used by people with malicious intent.

Keywords. Security, testing, attack, port, network, penetration.