УДК 004.056.5 + 004.7.056.5
ББК Х401.114

Косенко М. Ю.

СБОР ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

В работе рассматриваются основные фазы процесса проведения оценки безопасности компьютерных систем и сетей средствами моделирования атак злоумышленника. Предлагается модель распределенного сетевого сканирования, использующая в качестве платформы облачные технологии. Представленный метод повышает эффективность проведения тестирования на проникновение за счет сокращения времени, отводящегося на этап сбора информации.

Ключевые слова: *тестирование на проникновение, сканирование сети, облачные технологии.*

Kosenko M. U.

GATHERING INFORMATION DURING PENETRATION TESTING

The paper presents the main phases of process the evaluation security of computer systems and networks with simulation hackers attacks. Presents a model of distributed network scanning on cloud-based technologies. This method will increase the efficiency of penetration testing by reducing the time tailrace on information-gathering phase.

Keywords: *penetration testing, network scanning, cloud computing.*

1. Введение

В настоящее время при оценке безопасности компьютерных систем и сетей используются различные методы, один из которых – тестирование на проникновение. Тестирование на проникновение – это тестирование безопасности, в котором эксперты имитируют реальные атаки в попытке определить методы обхода функций безопасности приложения, системы или сети[1]. Тестирование часто включает в себя элементы реальных атак на системы, используя инструменты и методы, используемые злоумышленниками. Большинство тестов на проникновение включают в себя поиск комбинаций уязвимостей одной или нескольких систем, которые можно использовать, чтобы получить больший уровень доступа, чем может быть достигнуто с помощью одной уязвимости.

Тест на проникновение также может быть полезным для определения[2]:

• толерантности системы к шаблонам реальных атак;

• вероятного уровня сложности, при котором атакующий может успешно компрометировать систему;

• дополнительных контрмер, которые могли бы ослабить угрозы против системы;

• возможности защитников по обнаружению атак и реагированию соответствующим образом.

На рис. 1 представлены четыре фазы проведения тестирования на проникновение: планирование, сбор информации, атака, от-

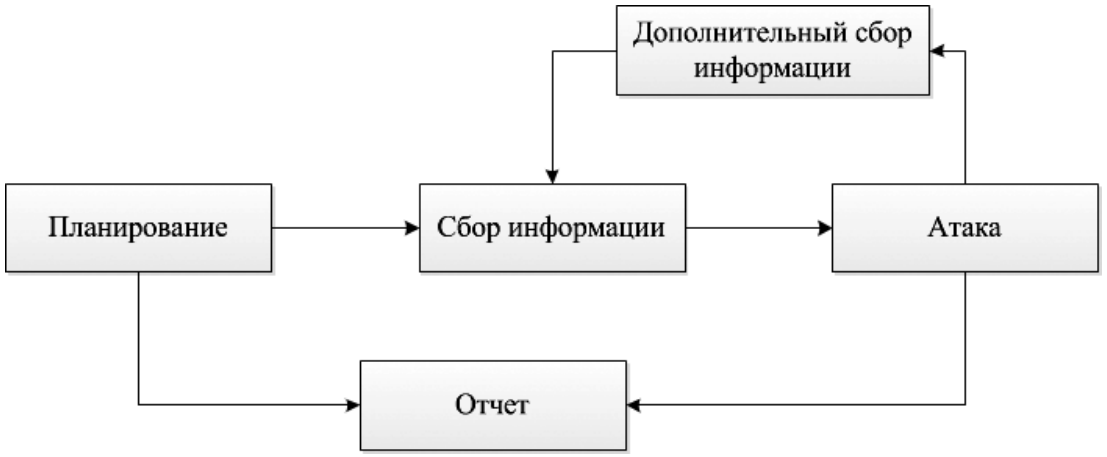

Рис. 1. Фазы проведения тестирования на проникновение.

чет. На этапе планирования определяются правила тестирования, документируется согласие руководства, устанавливаются цели. Данный этап определяет основу для проведения успешного теста на проникновение.

Фаза сбора информации состоит из двух частей. Первая часть является началом фактического тестирования и охватывает сбор общей информации о системе и сканирование. На этом этапе производятся обнаружение активных устройств в сети, открытых на них портов, и идентификация работающих служб. В дополнение могут использоваться другие методы сбора информации о целевой системе:

• Имена хостов и информация об IP-адресах может быть собрана различными методами, в том числе при опросе DNS, WHOIS запросах, прослушивании сети.

• Имена и контактная информация сотрудников может быть получена с помощью поиска на веб-сервере организации.

• Информацию о системе можно найти с помощью протокола NetBIOS или протокола информационной службы сети (Network Information Service, NIS).

• Информацию о приложениях и службах, такую, как номер версии, можно получить, используя метод «banner grabbing».

Вторая часть заключается в анализе уязвимостей и включает в себя автоматический поиск уязвимостей услуг, приложений и операционных систем отсканированных хостов, а также ручной поиск уязвимостей. Для выявления уязвимостей вручную эксперт может использовать свои собственные знания или общественные базы данных уязвимостей, таких как национальная база данных уязвимостей (National Vulnerability Database, NVD). Третий этап – основа теста на проникновение и включает в себя проведение атаки. Это процесс проверки ранее выявленных уязвимостей и попытка их эксплуатации. Фаза отчетности происходит одновременно с тремя другими фазами тестирования на проникновения. Отчет, как правило, разрабатывается для описания выявленных уязвимостей, представляет актуальные риски системы и дает указания о том, как смягчить обнаруженные слабые стороны.

Фаза атаки является основой любого теста на проникновение. Атака представляет процесс проверки выявленных уязвимостей путем их использования. Эта фаза включает в себя следующие шаги: получение доступа к системе, расширение привилегий, осмотр системы, установка в систему дополнительных инструментов.

Фаза отчетности происходит одновременно с тремя другими этапами. На этапе планирования разрабатывается и описывается план действий. На этапе сбора информации и атаки ведется журнал работы. По завершении теста на проникновение в отчет заносится описание выявленных уязвимостей и даются рекомендации по устранению обнаруженных недостатков.

Первая часть второй фазы проведения тестирования на проникновение, сканирование может занять большое количество времени, особенно если стоит задача просканировать большую сеть. Таким образом, при реализации этого этапа становится актуальной возможность параллельно распределить трафик к сканируемым хостам.

2. Модель распределенного сканирования сетей

Целью данной работы является разработка инструмента, позволяющего создавать и управлять множеством хостов, имеющих свой собственный канал для сканирования исследуемой сети.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Построить концептуальную модель распределенного сканирования сети.

2. Разработать алгоритм работы системы распределенного сканирования.

3. Проанализировать инструменты сканирования сети.

4. Разработать инструмент распределенного сканирования.

2.1. Описание модели

Сетевое сканирование является отправной точкой в тестировании на проникновение. Цель этого процесса состоит в определении числа достижимых систем для тестирования, их IP-адресов, открытых портов, идентификации работающих сервисов и операционных систем[3]. За последние пару десятков лет сканирование очень сильно развилось и было разработано множество методов его проведения[4]. Если рассматривать технологии сетевого сканирования с точки зрения многоуровневой модели TCP/IP, то существует достаточно много техник: сканирование на уровне 2, ICMP-сканирование, UDP-сканирование, TCP-сканирование (различные варианты SYN, ACK, FIN)[5]. Каждая из этих технологий наилучшим образом применима в различных ситуациях, связанных с настройкой сканируемых хостов.

Для размещения системы распределенного сканирования сети можно использовать облачную модель предоставления услуг – инфраструктура как услуга (Infrastructure as a Service, IaaS)[6]. Данная услуга позволяет за короткие сроки развернуть в сети множество подконтрольных виртуальных машин. Используя возможности, предоставляемые сервисом IaaS, можно обходить различные защитные средства, такие как Intrusion detection system (IDS, система обнаружения вторжений) или Intrusion prevention system (IPS, система предотвращения вторжений). Такая возможность появляется за счет того, что сканирование может происходить с десятка различных IP-адресов, выдерживая временные интервалы.

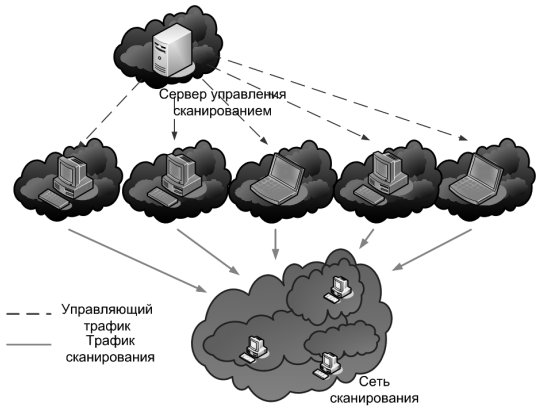

Рис. 2. Концептуальная модель распределенного сканирования с использованием облачных технологий

На рис. 2 представлена концептуальная модель распределенного сканирования. Компонентами этой модели являются:

• клиенты, осуществляющие сканирование (скан-бот). Виртуальные машины, выполняющие функцию сканирования. По окончании выполнения команды скан-бот передаёт результаты сканирования серверу управления;

• сервер управления сканированием. Виртуальная машина, выполняющая функцию управления скан-ботами. Скан-боты соединяются с сервером управления сканированием и получают команды для выполнения;

• цель сканирования. Компьютерная сеть, либо отдельные компьютеры, которые нужно просканировать.

2.2. Алгоритм системы распределенного сканирования

Создать систему распределенного сканирования можно, используя модель взаимодействия клиент/сервер[7]. В таком случае алгоритм работы системы распределенного сканирования будет следующим.

1. Сервер управления сканированием запускается и загружает задачи сканирования из заранее заполненного лицом, проводящим тестирование, файла. В данном файле приводится список всех задач, которые необходимо распределить по скан-ботам.

2. Скан-бот осуществляет подключение к серверу. При запуске скан-бота в качестве параметров передаются адрес и порт сервера управления сканированием.

3. При подключении нового скан-бота сервер выдает ему очередное задание, ожидающее выполнения.

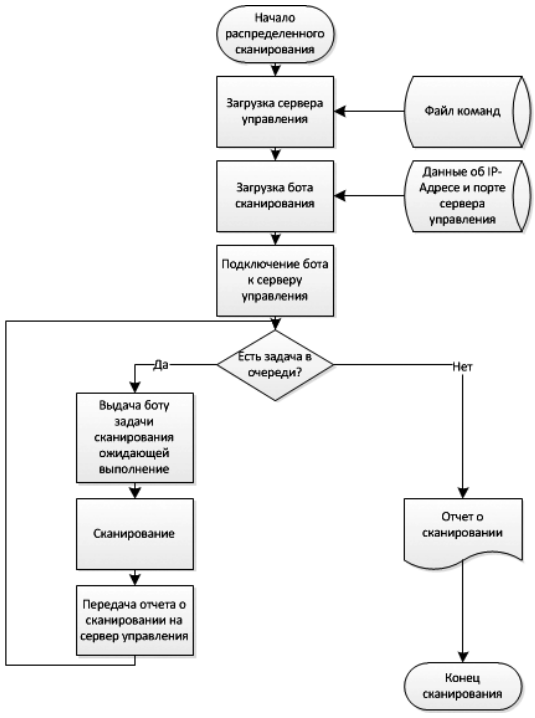

Рис. 3. Блок-схема алгоритма распределенного сканирования

4. Скан-бот выполняет задание. Результат передает серверу управления сканированием.

5. Сервер управления агрегирует полученную информацию сканирования в специальном каталоге. При наличии ожидающей выполнения задачи передает её освободившемуся скан-боту.

Блок-схема алгоритма работы системы распределенного сканирования приведена на рис. 3.

2.3. Реализация системы распределенного сканирования

В качестве облачного провайдера был выбран DigitalOcean, предоставляющий облачную модель инфраструктуры как услуги. С использованием сервиса DigitalOcean были созданы два образа виртуальной машины. Первый образ был подготовлен в качестве сервера управления сканированием. Второй образ включал все необходимые компоненты для осуществления сканирования. Сервис DigitalOcean позволяет быстрым образом запускать множество клонов созданной виртуальной машины.

Для сканирования использовался сетевой сканер Nmap. Nmap ("Network Mapper") – это программа с открытым исходным кодом для исследования сети и проверки безопасности[8]. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Данный сетевой сканер выбран потому, что обладает рядом преимуществ перед другими сканерами:

• Гибкость. Nmap включает в себя множество механизмов сканирования портов, обнаружение операционной системы, определение версий служб.

• Мощность. Nmap может быть использован для сканирования огромных сетей, состоящих из сотен тысяч машин.

• Кроссплатформенность. Большинство операционных систем поддерживают Nmap, включая Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, MacOS, NetBSD и др.

Серверное и клиентское программное обеспечение системы распределенного сканирования было реализовано с использованием языка программирования Python. Помимо основных задач, сервер, используя пакет python-digitalocean, обеспечивающий простой доступ к DigitalOcean API, имеет возможность запуска виртуальных машин скан-ботов в облачной инфраструктуре. Количество запускаемых виртуальных машин определяется согласно количеству задач в очереди сканирования.

3. Заключение

В рамках представленной работы были достигнуты следующие результаты:

• описана модель распределенного сканирования сети;

• разработан алгоритм работы системы распределенного сканирования;

• реализована система распределенного сканирования на базе облачных технологий.

Разработанная система повышает эффективность проведения теста на проникновение за счет сокращения времени, отводящегося на этап сбора информации.

Примечания

[1] Thomas Wilhelm. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab". Syngress, 2009.

[2] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. "Technical Guid to Information Security Testing and Assessment". NIST Special Publication 800–115.

[3] Pete Herzog. "Open-Source Security Testing Methodology Manual". ISECOM, 2006.

[4] M. Allman, V. Paxson, and J. Terrell. "A brief history of scanning". In IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, 2007, pp 77–82.

[5] Richard J Barnett, Barry Irwin. "Towards a Taxonomy of Network Scanning Techniques". In SAICSIT, 2008.

[6] Косенко М. Ю. Злонамеренное использование облачных технологий. Труды Первой Международной конференции «Информационные технологии и системы». 2012. с. 67–69.

[7] Douglas E. Comer, David L. Stevens. "Internetworking with TCP/IP. Vol III. Client-Server Programming and Applications Linux/POSIX Socket Version". Addison-Wesley, 2000.

[8] Gordon Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning". Nmap Project, 2009.

[9] James Messer. "Secrets of Network Cartography: A Comprehensive Guide to Nmap".

[10] Chris McNab. "Network Security Assessment". O'Reilly Media, Second Edition, 2007.

[11] "Penetration Testing: Procedures & Methodologies". EC-Council, 2010.

References

[1] Thomas Wilhelm. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab". Syngress, 2009.

[2] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. "Technical Guid to Information Security Testing and Assessment". NIST Special Publication 800-115.

[3] Pete Herzog. "Open-Source Security Testing Methodology Manual". ISECOM, 2006.

[4] M. Allman, V. Paxson, and J. Terrell. "A brief history of scanning". In IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, 2007, pp 77-82.

[5] Richard J Barnett, Barry Irwin. "Towards a Taxonomy of Network Scanning Techniques". In SAICSIT, 2008.

[6] Kosenko M.Yu. Zlonamerennoe ispol'zovanie oblachnykh tekhnologii. Trudy pervoi mezhdunarodnoi konferentsii «Informatsionnye tekhnologii i sistemy» [Use of cloud technologies for malicious purposes. Materials of the international conference 'Information technologies and systems]. 2012. p.67-69.

[7] Douglas E. Comer, David L. Stevens. "Internetworking with TCP/IP. Vol III. Client-Server Programming and Applications Linux/POSIX Socket Version". Addison-Wesley, 2000).

[8] Gordon Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning". Nmap Project, 2009.

[9] James Messer. "Secrets of Network Cartography: A Comprehensive Guide to Nmap".

[10] Chris McNab. "Network Security Assessment". O'Reilly Media, Second Edition, 2007.

[11] "Penetration Testing: Procedures & Methodologies". EC-Council, 2010.

Косенко Максим Юрьевич, преподаватель института информационных технологий Челябинского государственного университета. г. Челябинск, ул. Братьев Кашириных, 129, к. 415. E-mail: kosenko@csu.ru

Maksim Yurievich Kosenko, lector and teacher of the Institute of Informational Technologies of Chelyabinsk State University. Office 415, Bratiev Kashyrinykh Str., Chelyabinsk. E-mail: kosenko@csu.ru