Е.И. Бруев, Е.А. Оленников

Тюменский государственный университет, г. Тюмень
УДК 004.451

АВТОМАТИЗИРОВАННАЯ ПОДГОТОВКА ВИРТУАЛЬНЫХ МАШИН С ЗАДАННЫМИ УЯЗВИМОСТЯМИ НА БАЗЕ ГИПЕРВИЗОРОВ VMWARE PLAYER и VSPHERE

Аннотация. Развертывание виртуальных машин задача тривиальная, но, когда необходимо массово создавать разные виртуальные машины с разными операционными системами задача не простая. С помощью средств автоматизации возможна массовая подготовка и интегрирование программного обеспечения. В результате возможно подготовить инструменты – исполняемые файлы для автоматизированной развертки одной или нескольких виртуальных машин с программными уязвимостями.

Ключевые слова: VMware, ESXi, vSphere, Гипервизор, Виртуализация, Скрипт, Пентест.

Тестирование на проникновение становиться все более востребованной задачей. Это сложная и трудоемкая работа, для проведения которой необходимо обладать большим числом компетенций, владеть различными техниками, иметь обширные знания в различных областях. Подготовка таких специалистов является актуальной задачей.

Очевидно, что процесс обучения таких специалистов должен включать большой объем практической работы, в процессе которой обучаемый должен получить реальный опыт проведения пентеста в условиях максимально приближенных к реальным.

Учитывая тот факт, что реальными объектами для проведения пентеста, как правило, являются корпоративные сети во всем их многообразии, где используются разные ОС с их вариативностью версий и сборок, а также различное программное и аппаратное обеспечение, обладающее, возможно,

уникальным набором уязвимостей. Воссоздать такую инфраструктуру на базе прохождения обучения весьма проблематично, а это:

1) большие затраты по времени;
2) большой объем затрачиваемых ресурсов;
3) калибровка и отладка процессов;
4) постоянное переключение типов задач.

В связи с этим для кафедры информационной безопасности Тюменского государственного университета было предложено решение, с использованием средств автоматизации, на основе сценариев, развернуть виртуальную, изолированную, среду для проведения учебных занятий по тестированию на проникновение.

Решить эту проблему помогут современные технологии виртуализации и инструменты автоматизации процессов.

На рынке свободного программного обеспечения уже существует приложение Secure Scenario Generator [1], разрабатываемое Клифом Шройдером, позволяющее развернуть виртуальную машину с набором уязвимостей при использовании инструмента Vagrant [2].

Использование данного приложения для реализации на гипервизоре vSphere нецелесообразно на основании ряда факторов:

1) не полная поддержка гипервизора ESXi;
2) отсутствие поддержки vSphere;
3) сложность развертывания ОС семейства Windows;
4) использование одних и тех же ОС для развертки;
5) использование большого объема зависимых пакетов;
6) для массового развертывания ВМ необходима БД.

Взамен было предложено альтернативное решение с использованием свободно распространяемого инструмента Packer. С помощью данного инструмента возможно разворачивать ОС с нуля с использованием скриптов, а также, с помощью дополнительных плагинов, обращаться к API гипервизора vSphere [3].

Для поддерживаемых версий Windows и Windows Server создаются специальные конфигурации на разметке XML, позволяющие пропустить мастер установки, путем автоматического ввода необходимых параметров.

Для Unix-Like систем, в частности Debian, CentOS 7 и Ubuntu создаются скрипт с загрузочными командами, позволяющие установить ОС в автоматическом режиме.

Таким образом, можно использовать любые поддерживаемые версии ОС обоих семейств, а также использовать разные версии их сборок, что повышает разнообразие будущей инфраструктуры.

Для того, чтобы интегрировать уязвимое ПО в ОС необходимо воспользоваться методом написания скриптов с помощью штатных инструментов: Bash, sh или PowerShell, Batch.

Для семейств Windows, подготовка одной ВМ разделяется на три этапа:

1. Установка ОС;

2. Подключение необходимых инструментов, в частности OpenSSH клиент, необходимый для развертывания и передачи по нему дополнительного софта, согласно сценарию.

3. Выполнение развертывания согласно сценарию.

Для Unix-Like систем, в силу ее богатого инструментария «из коробки», подготовка одной ВМ разделяется на два этапа:

1. Установка ОС;

2. Выполнения развертывания согласно сценарию.

Для управления всеми скриптами и средствами автоматизации, администратор должен знать метод установки ОС, порядок установки, затрачиваемое время подготовки того или иного пункта, например: время подготовки к установке и т.п. Это обусловлено тем, что процесс подготовки ОС с ее установкой, работает на основе командной оболочки, которая и выполняет заданные администратором аргументы, будь то графический интерфейс или командная строка, ведь для сценария, важным фактором является последовательность выполнения команд.

Сценарии состоят из аргументов, написанных на языке разметки XML и структуре JSON для Windows и JSON и Config File для Unix-like. Они содержат необходимые аргументы и команды, задаваемые администратором, с помощью которых применяется нужное значение для установки, настройки и эксплуатации ОС.

С помощью сценариев дается возможность создать виртуальные дисководы, в которые помещаются исполняемые файлы для дальнейшей настройки ОС. Часть скриптов для выполнения процессов помещаются в них, особенно когда скрипты зависимы друг от друга, создавая тем самым буферную зону, где сценарий ожидает их завершения.

Также, стоит учитывать, что при автоматизированной разведке на основе гипервизора первого уровня могут возникнуть ряд проблем, связанные с ограничением доступа или отсутствием его вовсе для конкретного модуля, что усложняет подготовку виртуальной инфраструктуры, в отличии от гипервизоров второго уровня, где администратор имеет полный доступ к его инструментарию.

Заключение

Процесс создания виртуальных машин с последующей автоматизированной установкой программного обеспечения весьма быстр и надежен. Грамотное владение скриптовыми языками PowerShell и Shell обеспечивают автономность выполнения процессов без участия администратора. Таким образом, соединение нескольких сценариев позволяет подготовить большое количество ВМ и интегрировать в них программное обеспечение, а также различные программные уязвимости.

СПИСОК ЛИТЕРАТУРЫ

1. Schreuders C. GitHub [В Интернете]. – 2021 г. – 1 марта 2021 г. – URL: https://github.com/cliffe/SecGen/ (дата обращения: 20.04.2021).

2. Schreuders Z. Cliffe Episode 011 – Security Scenario Generator with Dr. Z. Cliffe Schreuders [Интервью]. – 17 ноября 2017 г.

3. VMware SDK_PUBS. Documentation. [В Интернете]. – URL: https://www.vmware.com/support/pubs/sdk_pubs.html

4. Ardern Z. Cliffe Schreuders and Lewis Generating randomised virtualised scenarios for ethical hacking and computer security education [Журнал] // Vibrant Workshop 2015. – Leeds, UK : Leeds Beckett University, 2015.

5. Schreuders Z.C., Shaw T., Mac Muireadhaigh A., Hackerbot P.S. Attacker Chatbots for Randomised and Interactive Security Labs, Using SecGen and oVirt [Журнал] // USENIX Association. – Балтимор, США : Leeds Beckett University, 2018. – С. 1-10.

6. Schreuders Z.C., Shaw T., Shan-A-Khuda M., Ravichandran G., Keighley J., Ordean M. Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events [Журнал] // USENIX Association. – Ванкувер, Канада : Leeds Beckett University, University of Birmingham, 2017.