ХАКИНГ [ЛЕКЦИЯ 6]

Добыча VDS-серверов (Дедиков), используя Metasploit Framework

В этой лекции я покажу тебе метод добычи удаленного дедика под управлением Windows средствами Metasploit Framework с использованием уязвимости MS08-067. Почему-то эксплуатация этого бага в настоящее время пользуется большой популярностью среди хакеров, о чем свидетельствуют многочисленные записи и обсуждения в Facebook , хотя на страницах ВКонтакте, посвященных тому же самому MSF , царит полная тишина. В большинстве случаев уязвимыми являются все системы, работающие под управлением Windows XP Professional SP2 и SP3 (полный список операционок, подверженных риску, ты можешь найти на kb.cert.org/vuls/id/827267). Но на самом деле, все программные продукты Microsoft могут быть скомпрометированы путем эксплуатации данного бага и по сей день.

Перейдем к делу — качаем последний релиз Metasploit Framework на официальном сайте metasploit.com (или ищем на диске). Перед его установкой на компьютере отключаем антивирус. В комплект Metasploit Framework включен свой собственный сетевой сканер портов, хотя для поиска подключенных к сети машин под управлением ОС Windows мы можем использовать и внешний сканер **nmap**, который также добавлен в дистрибутив и устанавливается одновременно с Metasploit Framework.

1. Запускаем сканер nmap, отметив порт 445, поскольку именно он нам и нужен для дальнейшей эксплуатации уязвимости службы сервера. А что, собственно, мы будем сканировать? Ответ достаточно прост — например, можно взять и просканировать IP-префиксы своего провайдера, которые мы с легкостью узнаем на сайте bgp.he.net в разделе «Prefixes IP v4».

Для использования полученных префиксов в сканере nmap, необходимо их предварительно скопировать в файл — например, my_isp.txt, и поместить файл в рабочий каталог с nmap.

2. Команда запуска сканера будет выглядеть следующим образом:

```
nmap -T4 -A -v -PE -PS445 -PA445 -iL my_isp.txt
```

Отлично, в результате сканирования мы получили список хостов с запущенной службой сервера, которую видно из внешней сети, причем она ничем не прикрыта, хотя Microsoft еще в 2008 году настоятельно рекомендовали блокировать доступ из интернета к этому сервису… Интересно, что по каждому хосту nmap выдает подробную информацию о типе установленной ОС.

Виды shell: полезная нагрузка meterpreter и другие

В настоящее время считается, что полнофункциональный Meterpreter (MP) существует только под Windows, но на самом деле это не совсем так. Существует еще несколько версий MP, реализованных на PHP и JAVA. Впрочем, ты и сам можешь стать автором «полезной нагрузки» — например, скомпилировать TCL-сценарий shell-кода для Cisco IOS с помощью утилиты tclpro.exe и в дальнейшем использовать его для жестоких игр с железными кошками

Стандартную полезную нагрузку MP можно использовать почти со всеми Windows-эксплойтами, включенными в Metasploit Framework, выбрав одну из следующих полезных нагрузок:

Кратко поясню суть каждой.

1. **bind_meterpreter**— резервирует порт на целевой машине и ожидает соединения. После установления соединения происходит загрузка Meterpreter’a на целевой хост, текущее соединение продолжает использоваться для связи с удаленной машиной.
2. **reverse_meterpreter**— сама соединяется с предварительно заданным хостом по указанному порту для дальнейшей загрузки Meterpreter’a. Затем установленное соединение используется для связи с удаленной машиной. Все хорошо, но для успешной реализации данного метода нам понадобится

реальный IP-адрес (или устанавливай проброс нужных тебе портов через NAT).

3. **find_tag**— осуществляет поиск дескриптора службы, обработанной эксплойтом, и использует его для загрузки Meterpreter’а на удаленную машину, после чего существующее соединение будет использовано для связи с ней. Этот вид полезной нагрузки является особенно интересным, поскольку тут не требуется открывать новое соединение — таким образом, существует возможность обхода практически любых конфигураций брандмауэров.
4. **bind_tcp**— это обычный командный интерпретатор типа cmd.exe, естественно, без всяких дополнительных наворотов, как у Meterpreter`a. Он просто резервирует порт на целевой машине и загружает стандартную оболочку.

В зависимости от цели исследования системы может быть использована любая из этих полезных нагрузок. Так чего же мы ждем? Выбираем цель из списка, полученного в результате сканирования nmap, и подключаемся к ней. Для простоты эксперимента будем использовать простой командный интерпретатор в качестве полезной нагрузки.

```
msf > use exploit/windows/smb/ms08_067_netapi

msf exploit> set PAYLOAD windows/vncinject/bind_tcp

PAYLOAD => windows/vncinject/bind_tcp

msf exploit(ms08_067_netapi) > set RHOST 192.168.0.3

RHOST => 192.168.0.3

msf exploit(ms08_067_netapi) > exploit
```

Если уязвимость на удаленной машине существует, то мы получим доступ к шеллу (cmd.exe) этого компьютера, и в окне появится сообщение о том, что

сессия успешно установлена. В случае, когда msf определил ОС как Windows 7, можно попробовать использовать 64-разрядные полезные нагрузки, которые имеются в соответствующем разделе (ищем через меню GUI), или вызвать нагрузку через консоль. Пример работы эксплойта с полезной нагрузкой можно посмотреть на видео (ищи ролик на нашем диске).

Захват сервера

Теперь из списка хостов, сгенерированных nmap, выберем IP-адрес под управлением ОС Windows 2003 Server — это и будет наша искомая цель (ведь ты, как настоящий сетевой гуру, хотя бы раз в жизни должен поиметь свой собственный дедик!). Для работы с сервером будем использовать все тот же эксплойт (exploit/windows/smb/ms08_067_netapi) и полезную нагрузку bind_meterpreter. В результате мы получаем доступ к командной оболочке через Meterpreter, после чего добавляем нового пользователя с помощью сценария token_adduser, предварительно повысив свои привилегии на удаленной машине до уровня SYSTEM с помощью команды use priv. Ну вот — у нас есть дедик, к которому ты можешь подключаться, используя удаленный рабочий стол. На нем мы можем установить прокси-сервер, FTP и многоемногое другое. В ходе эксперимента у меня получилось набрать пять дедиков примерно в течение часа. Я думаю, это круто!

Заключение

Если кто-то хочет просто жать на кнопку «exploit», чтобы Metasploit сразу выдавал готовые дедики, то скажу сразу — этого не будет: метод все равно требует времени и терпения.

Атака из локальной сети, скорее всего, приведет к тому, что система будет полностью скомпрометирована. Несмотря ни на что, все еще остается довольно широкое поле для экспериментов с безопасностью Windows, и ты можешь внести свой вклад в это дело ☺