

ИСПОЛЬЗОВАНИЕ RDP ДЛЯ НАПАДЕНИЯ

Стасивский Л.С.

ГВУЗ «Национальный горный университет», <http://bit.nmu.org.ua>, stasivskyj@gmail.com

Появление любой технологии сулит чаще всего и новые специфические проблемы. Конечно, терминальные службы Microsoft – понятие совсем не новое, тем не менее использовать ее в хакерских целях может быть очень даже интересно. Итак, предположим, что злоумышленник должен атаковать какую-то корпоративную сеть, а точнее, ее пользователей.

Ключевые слова – протокол удалённого рабочего стола; защита POP-сервер.

Remote Desktop Protocol (RDP, протокол удалённого рабочего стола) позволяет пользователям удаленно работать на хосте, используя нативный графический интерфейс. Но как можно атаковать пользователей, обладая доступом к POP-серверу? Самый простой вариант лежит в возможности автоматического монтирования дисков и устройств клиента при подключении к POP-серверу. То есть при подключении пользователя к POP-серверу диски становятся доступными для POP- сервера и у него появляется возможность поместить на клиент любые файлы в любое место (в зависимости от прав пользователя в своей ОС). Конечно, по умолчанию диски не монтируются, но здесь есть некоторые тонкости.

Во-первых, через стандартный POP-клиент (mstsc) нет возможности задавать, при подключении к какому серверу монтировать диск, а к какому – нет. Там используются общие настройки для всех подключений. Таким образом, достаточно часто получается, что администраторы “ходят” на POP по серверам с подключенными дисками, и это создает

прекрасную основу для атаки. По сути, нужно захватить контроль над одним из серверов и тем или иным образом заставить администратора зайти на него, а далее все информация становится доступной.

Во-вторых, можно принудительно включить опцию подключения дисков – за счет указания соответствующих настроек в POP- файлах. И это дает несколько иной вектор атаки – атаку на офисных пользователей. Суть заключается в том, что злоумышленник может создать такой POP-файл, при запуске которого у пользователя ничего спрашивать не будет, а автоматически произойдет подключение к RDP-серверу с автоматическим монтированием дисков и последующим захватом контроля пользовательским компьютером. Конечно, здесь потребуется проявить немного социальной инженерии. Например, можно разослать офисным работникам письма с приложенными POP-шками и просьбой их запустить для тестирования какой-то новой системы. Такие файлы не вызовут подозрения у офисных работников, и, большинство выполнит необходимые действия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Обновление возможностей Remote Desktop Services в Windows Server 2012. (Электрон. ресурс) / Способ доступа: URL: <http://habrahabr.ru/company/microsoft/blog/167289> - Обновление возможностей Remote Desktop Services в Windows Server 2012.

2. Remote Desktop Protocol (RDP). (Электрон. ресурс) / Способ доступа: URL: http://en.wikipedia.org/wiki/Remote_Desktop_Protocol – Remote Desktop Protocol (RDP).