Атака SMB Relay и как от этого защититься

spy-soft.net/smb-relay

19 марта 2017 г.

Если в сети используются протоколы NBNS и LLMNR, это открывает возможность не только для атак с целью перехвата хешей паролей пользователей, но и для хорошо известной атаки **SMB Relay**.

Этот метод позволят нарушителю перехватить аутентификациинные данные, передаваемые от одного узла к другому, в процессе обмена информацией NTLM Challenge-Response.

Атака SMB Relay

Принцип атаки прост: нарушитель слушает сетевой трафик и ждет, когда один из узлов инициирует подключение к другому узлу. Как только такой запрос обнаружен, нарушитель реализует атаку «человек посередине» (например, LLMNR Spoofing): перехватывает запрос на аутентификацию от обратившегося узла и передает его на атакуемый сервер. Этот сервер возвращает ответ — просьбу зашифровать некоторое сообщение с помощью своего хеша, после чего перенаправляет его на узел, запросивший подключение. Следом происходит перенаправление этого зашифрованного сообщения. Так как сообщение было зашифровано корректным хешем, атакуемый сервер отправит нарушителю разрешение на аутентификацию. Злоумышленник аутентифицируется на сервере, а узлу, запросившему аутентификацию, отправит ответ об ошибке подключения. Нарушитель может реализовать такую атаку и в отношении того же ресурса, который отправляет запрос на подключение.

Эта атака известна давно, и компания Microsoft еще в 2008 году выпустила бюллетень безопасности MS08-068 и соответствующий патч для Windows. На системе с патчем нарушитель не сможет провести атаку на тот же компьютер, если

он инициирует подключение. Но возможность атаковать с помощью SMB Relay другие узлы в домене останется, если на них не реализована подпись SMB-пакетов — SMB Signing.

Простоту реализации атаки покажем на примере одного из наших пентестов. Анализируя трафик сети, мы выявили, что один из компьютеров периодически запрашивает адрес другого узла, после чего шлет на него HTTP-запрос с доменной учетной записью. С помощью утилиты Responder мы успешно атаковали выбранный нами узел сети, отправив запрос на подключение с того узла, который изначально инициировал запрос.

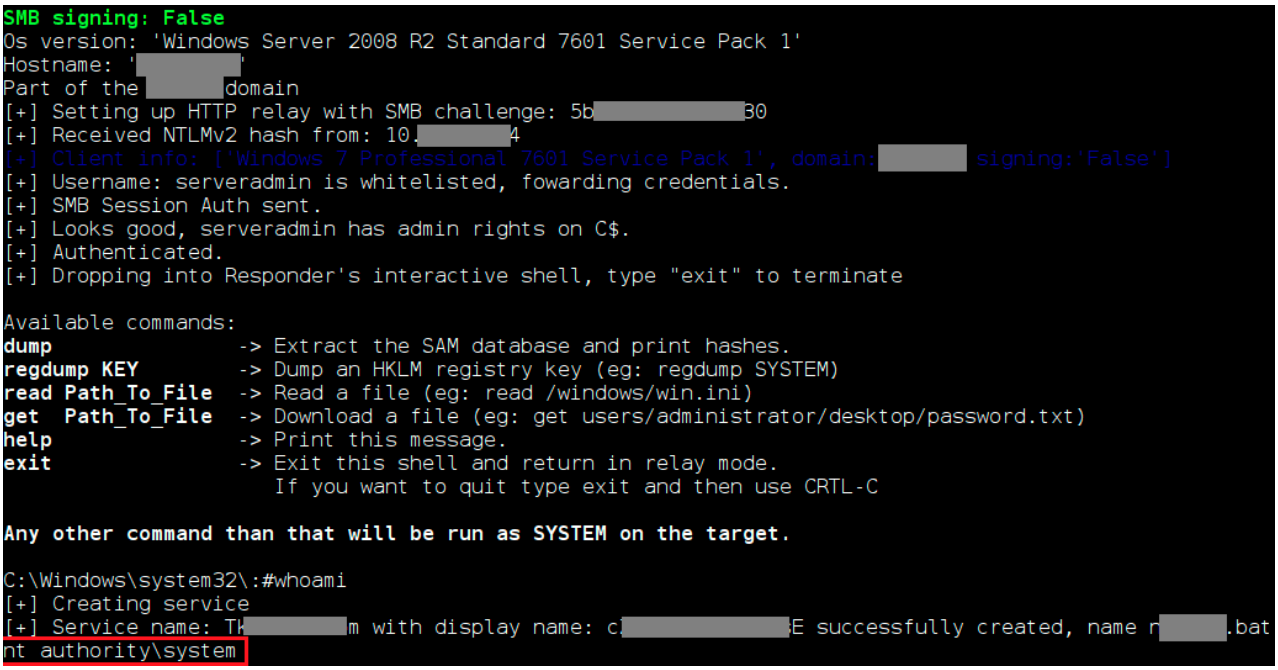
```
[+] HTTP Options:
    Always serving EXE          [OFF]
    Serving EXE                 [OFF]
    Serving HTML                [OFF]
    Upstream Proxy              [OFF]

[+] Poisoning Options:
    Analyze Mode                [OFF]
    Force WPAD auth             [OFF]
    Force Basic Auth            [OFF]
    Force LM downgrade          [OFF]
    Fingerprint hosts           [ON]

[+] Generic Options:
    Responder NIC               [eth0]
    Responder IP                [10.       1]
    Challenge set               [1122334455667788]
    Respond To                  ['10.         4']
    Don't Respond To Names      ['       ']


[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.       4 for name
[FINGER] OS Version     : Windows 7 Professional 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Professional 6.1
[*] [LLMNR]  Poisoned answer sent to 10.       4 for name
[FINGER] OS Version     : Windows 7 Professional 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Professional 6.1
[*] [LLMNR]  Poisoned answer sent to 10.       4 for name
[FINGER] OS Version     : Windows 7 Professional 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Professional 6.1
[+] Exiting...
```

На атакованном сервере возможно выполнение команд с привилегиями того пользователя, чьи аутентификационные данные были перехвачены в рамках SMB Relay (в нашем случае привилегии оказались максимальными). В результате был получен полный контроль над сервером.



Вероятность реализации подобной атаки высока. В крупных сетевых инфраструктурах часто используются автоматические системы для инвентаризации ресурсов, установки обновлений, резервного копирования и других задач. Такие системы ежедневно подключаются к ресурсам домена и могут использоваться нарушителями для атак.

Защита от атаки SMB Relay

Для защиты от атаки необходимо реализовать подписывание SMB-пакетов (SMB Signing) на всех узлах сети, а также отключить протоколы NBNS и LLMNR.

Кроме того, необходимо регулярно устанавливать актуальные обновления безопасности ОС.

Видео: Атака SMB Relay