????? ??????????? ???????

Применение эксплойтов

Самыми распространенными уязвимостями Windows машин в разное время являлись:

CVE-2008-4250 (MS08-067)
CVE-2017-0143 (MS17-010)
CVE- 2019-0708 (BlueKeep)

-----> полный список

MS08-067

MS08_067_netapi — один из самых популярных удаленных эксплойтов против Microsoft Windows. Он считается надежным
эксплойтом и позволяет получить доступ как SYSTEM (это наивысшая привилегия Windows). В современных тестах на проникновение этот эксплойт, скорее всего, будет использоваться во внутренней среде и не так часто. Во внешней не так часто из-за вероятности наличия брандмауэра. Работает для:

- Windows 2000
- Windows XP
- Windows 2003

Эксплоит: Metasploit > exploits/windows/smb/ms08_067_netapi

MS17-010

MS17_010_eternalblue — удаленный эксплойт против Microsoft Windows, изначально написанный Equation Group (АНБ) и
разглашенный Shadow Brokers (неизвестной хакерской организацией). Он считается надежным эксплойтом и позволяет не только получить доступ как SYSTEM, но и полный контроль над ядром в кольце 0.

Что касается удаленных эксплойтов для ядра, этот эксплойт очень надежен и безопасен в использовании. Команда проверки также очень точна, поскольку патч Microsoft непреднамеренно добавил раскрытие информации с дополнительными проверками на уязвимые пути кода. Работает для:

- Windows XP x86 (All Service Packs)
- Windows 2003 x86 (All Service Packs)
- Windows 7 x86 (All Service Packs)
- Windows 7 x64 (All Service Packs)

- Windows 2008 R2 x64 (All Service Packs)
- Windows 8.1 x64
- Windows Server 2012 R2 x64
- Windows 10 Pro x64 (< Version 1507)
- Windows 10 Enterprise Evaluation x64 (< Version 1507)

Эксплоит: Metasploit > exploit/windows/smb/ms17_010_eternalblue

BlueKeep

Уязвимость BlueKeep была обнаружена в реализации протокола RDP в некоторых версиях ОС Windows в мае 2019. BlueKeep никак не относится к механизму работы самого протокола и затрагивает только его реализацию. В частности, уязвимость затрагивает часть кода, отвечающую за управление так называемыми виртуальными каналами (англ. virtual channels). Работает для:

- Windows 10
- Windows 7
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Эксплоит: Metasploit > exploit/windows/rdp/cve_2019_0708_bluekeep_rce

Атаки методом перебора

В каждой Windows машине есть по несколько протоколов, позволяющих реализовывать атаки на механизмы аутентификации. Небольшое понимание того, какие учетные данные и пароли использовать для подобных атак в определенном контексте, может сильно облегчить этот способ и сделать его крайне эффективным. Может быть атаковано:

- SMB
- MSSQL
- LDAP
- RDP

Пример атаки:

```
hydra -L ~/wordlists/user.txt -P ~/wordlists/pass.txt 192.168.1.5 smb -V
```

Подготовка
Перед тем, как провести атаку методом перебора, необходимо ответить на следующие вопросы:

- Можно ли узнать логины для пользователей в домене?
- Какие пароли использовать для подбора?
- Как не заблокировать пользователей в домене?

Словарь логинов

Словарь логинов из домена можно получить следующими способами:

- С этапа разведки;
- С внешних систем (почта);
- Скомпрометировав какую-либо машину / аккаунт: извлечь адресную книгу почты / получить доступ к LDAP
- Словарь паролей
- Словарь паролей можно подготовить, зная привычки / менталитет сотрудников компании. Самыми популярными паролями будут: Zima2023 , Vfhn2023 (Март2023), Company2023 и пр., т.е.: использование комбинаций года, месяца, имени компании и пр.

Словари нужно подбирать в соответствии с контекстом, в котором вы их используете.

Обход блокировки
Для обхода блокировки можно использовать атаку PasswordSpraying: 1 попытку подбора пароля для всех аккаунтов в списке в определенный период времени.

Особенность настройки систем Windows в том, что администраторы зачастую настраивают политику количества попыток ввода пароля. Обычно количество попыток в этой политике устанавливается в значение от 3-х до 10-ти раз в течение часа. В случае, если количество попыток превышено, аккаунт пользователя блокируется.

Перехват трафика и MitM-атаки на машины Windows

Особенность в использовании по умолчанию протоколов взаимодействия в локальной сети, через которые можно попытаться скомпрометировать каналы коммуникаций и получить доступ к управлению сеансами или данными в них. Каждый раз, когда машина Windows пытается выполнить разрешение доменного имени, она выполняет следующие действия:

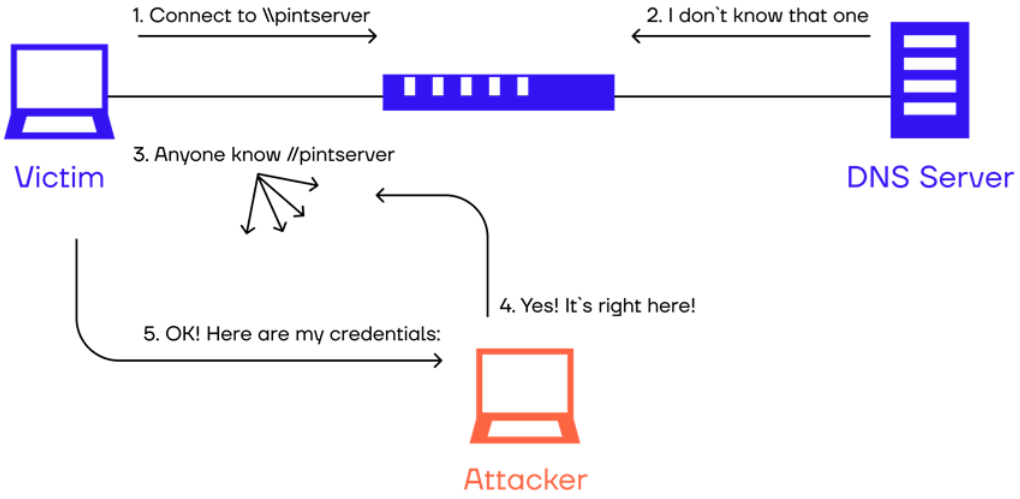
- Проверяет файл hosts для получения информации о системе и ее конфигурации
- Проверяет локальный кэш DNS
- Отправляет запрос к DNS
- Отправляет запрос LLMNR
- Отправляет запрос NBT-NS
- Отправляет запрос MDNS

Как раз в момент использования протоколов LLMNR, NBT-NS и MDNS становиться возможным подменить ответ на такой запрос и попытаться завести жертву на свой зловредный ресурс, который сможет:

- Направить жертву в сервис аутентификации и украсть хеш пароля аккаунта (а впоследствии — и сам пароль).
- Провести атаку Relay (захвата сеанса), выполнения команд от имени жертвы в машине, где она прошла аутентификацию, и пр.

LLMNR / NBT-NS / MDNS Spoofing.

В момент получения запроса LLMNR/NBT-NS можно подделать реальный источник разрешения имен в сети. Он отвечает на трафик так, как будто ему известна личность запрашиваемого узла: отправляет службу, чтобы жертвы общались с контролируемой системой.



Если узел, на который будет перенаправлена жертва, потребует прохождения процесса идентификации / аутентификации, имя пользователя и хэш NTLMv2 будут отправлены в контролируемую систему. Затем сохраняется хэш-информацию с помощью инструментов, отслеживающих трафик, далее взламываются хэши в автономном режиме методом грубой силы. Можно использовать NBNSpoof, Metasploit и Responder.

Responder

https://github.com/SpiderLabs/Responder

Responder — это инструмент для выполнения атаки MitM в отношении методов аутентификации в Windows. Эта программа
использует отправление LLMNR, NBT-NS и MDNS, через которое перенаправляет трафик с запросами и хешами аутентификации на подконтрольный узел.
Также в программу встроены серверы аутентификации HTTP/SMB/MSSQL/FTP/LDAP, которые поддерживают такие методы
аутентификации, как NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP и базовую HTTP аутентификацию. Для них
Responder выполняет роль ретранслятора.

Запустим Responder:

```
sudo responder -I eth0
```

Перехватив NTLMv2 хеш, положим их в файл tickets.txt и попробуем восстановить пароли аккаунтов, отправивших нам хеши:

```
hashcat -a 0 -w 4 -m 5600 tickets.txt /usr/share/wordlists/rockyou.txt
```

После получения пароля воспользуемся утилитой evil-winrm для получения удобного доступа к терминалу:

```
evil-winrm -i [ip] -u [username] -p [password]
```

Дополнительно

- Памятка по атакам MitM
- Телеграмм канал Магамы Базарова - эксперта по сетевым атакам
- Responder
- Все об атаках на аутентификацию в Windows
- О работе атаки NTLM Relay

Revision #2
Created 9 October 2025 18:16:21 by Admin
Updated 10 October 2025 08:06:19 by Admin