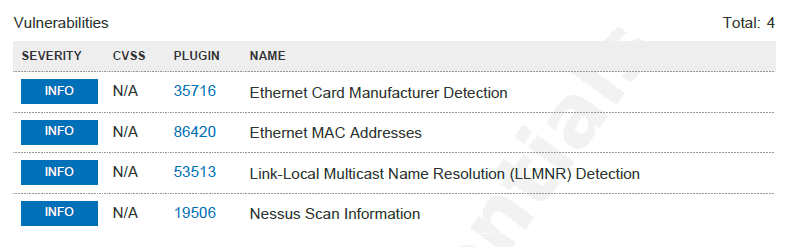
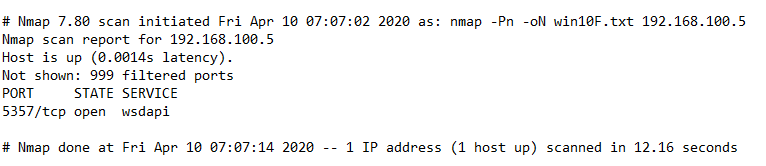
**Blue Teaming Aspect :**

Vulnerability Analysis :

Windows 10 met firewall :

Nessus heeft slechts 4 info vulnerabilities gevonden. De firewall doet hier dus uitstekend zijn werk.

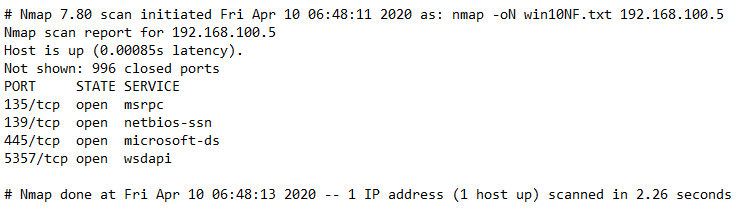
De Nmap scan heeft als resultaat ook slechts één open poort gevonden :

Deze poort kunnen we sluiten in de windows settings.

Windows 10 zonder firewall :

Zonder firewall vind Nessus veel meer vulnerabilities, hiervan is slechts één severe.

Doordat het signing niet nodig is kan de host te maken krijgen met een man in the middle aanval.

Het resultaat van Nmap heeft ook meer open poorten gevonden alhoewel het aantal nog meevalt.

Metasploitable3 :

Volgens de Nessus scan heeft deze host een totaal van 73 vulnerabilities. Ik ga enkel over de 5 critical vulnerabilities gaan.

Vulnerability in DNS Resolution Could Allow Remote Code Execution :

Door een fout in de versie van Windows kan men willekeurige code uitvoeren.

ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE :

De host’s web server heeft een Java applicatie die aangetast is door remote code execution.

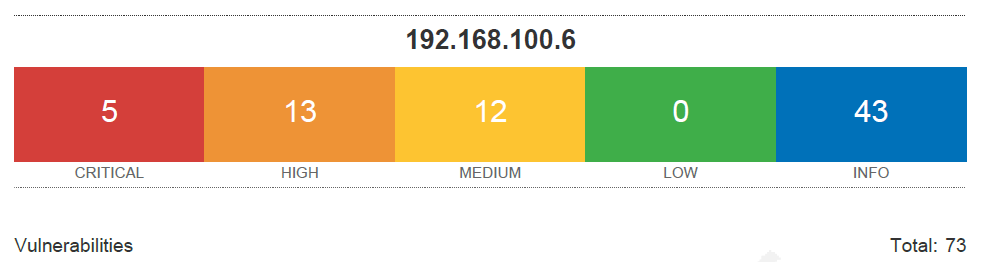
PHP 5.3.x < 5.3.15 Multiple Vulnerabilities :

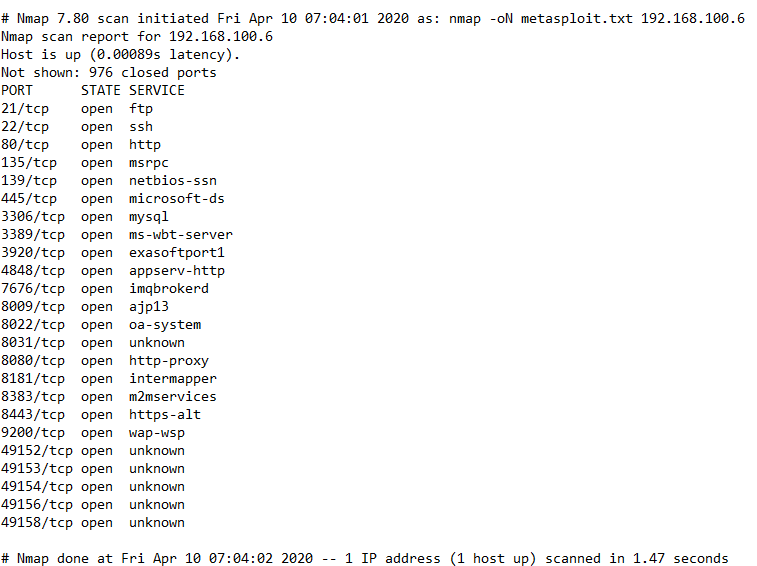
De host’s web server gebruikt een versie van PHP die mogelijk aangetast is.

PHP Unsupported Version Detection :

De host gebruikt een web scripting programmeertaal die niet meer word ondersteund.

Unsupported Windows OS

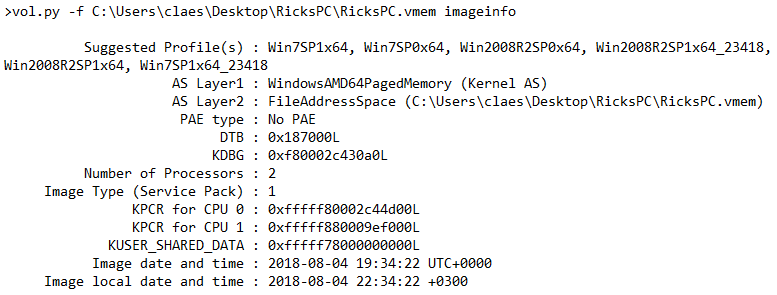
 De host’s versie van windows word niet meer ondersteund.

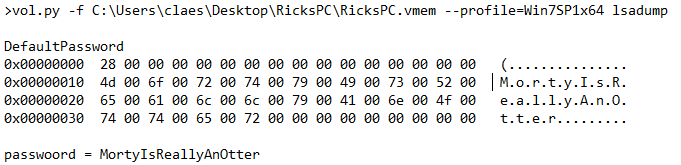
Ook de Nmap scan resulteert in 24 open poorten.

Forensics :

Rick’s PC :

Forensics software gebruikt: Volatility

Stap 1: Imageinfo ophalen

Resultaat: Win7SP1x64  
  
Stap 2: Wachtwoord ophalen

Resultaat: MortyIsReallyAnOtter

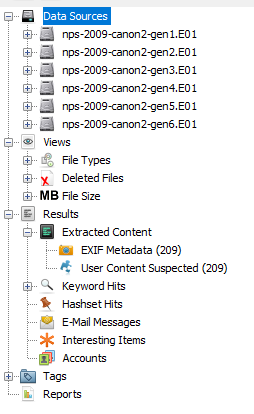
References:

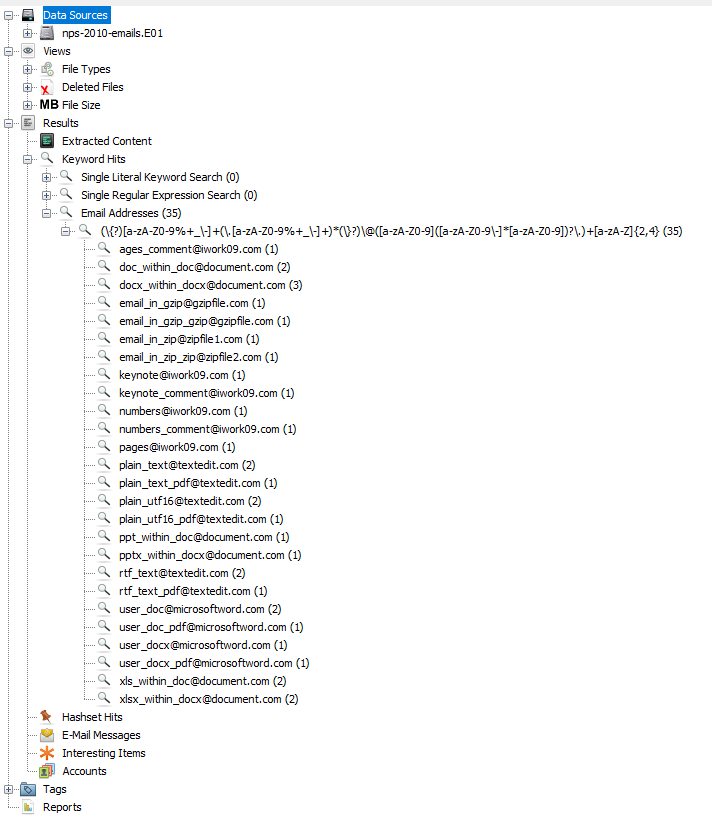
Blue Teams slides  
<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>

Forensics open :

Voorbeeld images DigitalCorpora: nps-2009-canon2, nps-2010-emails

Forensics software gebruikt: autopsy

Canon: EXIF Metadata > Handmatig de foto’s uithalen die gefixt zijn

Emails: Keyword hits > Email Adresses > 26/30 emails gevonden > laatste 4 handmatig in de  
files gezocht in de files die niet in de filter voorkomen

