# Basic Security Opdracht Systeem en Netwerkbeheer

## Nessus scan op Windows XP met firewall

De scan met firewall vond geen vulnerabilities, er werd wel aangegeven dat het een virtuele machine was.

## Nessus scan op Windows XP zonder firewall

De scan zonder firewall vond 7 vulnerabilities namelijk 4 kritieke, 1 hoge en 2 medium.

1. **Microsoft windows server 2003 unsupported installation detection.**

Dit wilt zeggen dat het Operating System verouderd is en niet meer ondersteunt word door Microsoft. Hier door krijgt het Operating System geen security updates meer en dit zorgt voor vulnerabilities.

**Oplossing:** Je Operating System updaten naar een nieuwere versie die wel ondersteunt wordt.

1. **MS06-040: Vulnerabiltiy in SSC Allow Cloud Allow Remote Code Execution.**

Dit wilt zeggen dat het mogelijk is dat er teveel data op korte termijn in de buffer van de server service geschreven wordt. Als deze exploit lukt krijgt de hacker volledige controle over het systeem.

**Oplossing:** Windows patches installeren

1. **MS08-067: Microsoft windows server service crafted RPC-request handling remote code execution.**

Dit wilt zeggen dat de server service RPC-requests slecht behandeld. Hierdoor kan een hacker via een aangepast RPC-request in het systeem geraken.

**Oplossing:** Windows patches installeren

1. **MS09-001: Microsoft Windows SMB2 vulnerabilities RCE3.**

Dit wilt zeggen dat de computer beïnvloed wordt door het ontregelen van het SMB-protocol. Een gevolg hier van kan het overnemen van het systeem of het afwijzen van services zijn.

**Oplossing:** Windows patches installeren.

1. **Dezelfde vulnerability als 2.**
2. **Microsoft windows SMB NULL session authentication.**

Dit wilt zeggen dat het mogelijk is om zonder gebruikersnaam en wachtwoord in te loggen op het system.

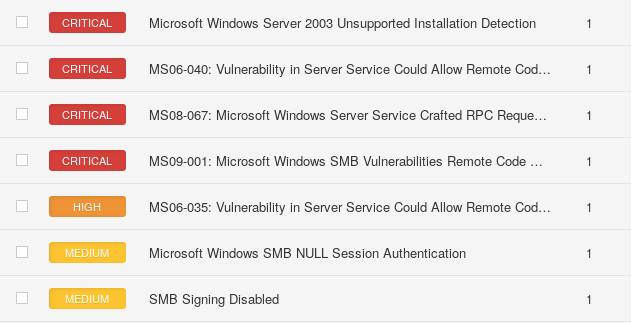
**Oplossing:** Pas de volgende veranderingen toe in het register (regedit):

* HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
* HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1   
  Remove BROWSER from :
* HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes Reboot once the registry changes are complete.
* Reboot your system

1. **SMB signing Disabled.**

Dit wilt zeggen dat het niet vereist is om te ondertekenen op de externe SMB server. Een gevolg hier van zijn dat een hacker een man-in-the-middle attack kan uitvoeren.

**Oplossing:** Aanpassen in de policy settings.



## OpenVas scan Windows XP met firewall

Hier kreeg ik een Internal error omdat OpenVas het target niet kan scannen als de firewall aanstaat.

## OpenVas scan Windows XP zonder firewall

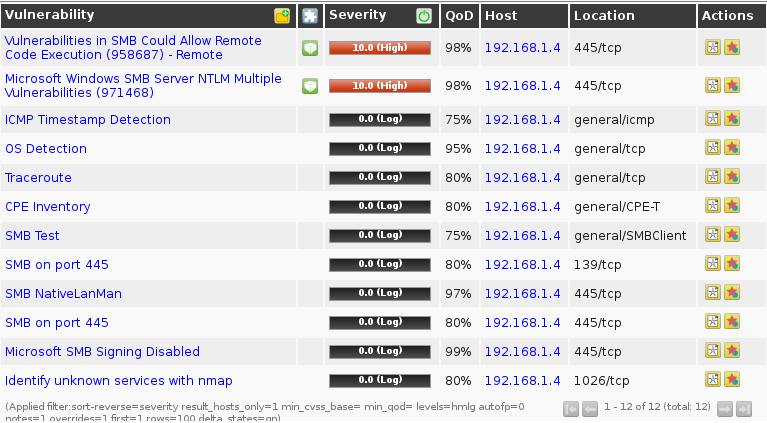
1. **MS09-001: Vulnerabilities in SMB could allow remote code execution – remote**

Dit wilt zeggen dat de computer beïnvloed wordt door het ontregelen van het SMB-protocol. Een gevolg hier van kan het overnemen van het systeem of het afwijzen van services zijn.

**Oplossing:** Windows patches installeren.

1. **MS10-012: Microsoft Windows SMB server NTLM multiple vulnerabilities.**

Dit wilt zeggen dat er een buffer overflow is via SMB pakketen (memory corruption). Een gevolg hier van kan denial of service zijn.

**Oplossing:** Windows patches installeren.

## Vergelijking Nessus en OpenVas

Eén van de eerste verschillen die mij opvalt is dat OpenVas niet kan scannen als de firewall aanstaat terwijl Nessus dit wel kan maar weinig of geen vulnerabilities vond. Nessus geeft ook meer vulnerabilities in vergelijking met OpenVas. Het is mij ook opgevallen dar Nessus sneller gaat onderverdelen in verschillende vulnerabilities dan OpenVas. OpenVas gaat deze meer beschrijven onder 1 vulnerability.

## Nessus scan Metasploitable OS (5 vulnerabilities)

1. **Rexecd service detection.**

Deze service zorgt ervoor dat gebruikers van een network op afstand commando’s kunnen uitvoeren.

**Oplossing:** Je moet de “exec” lijn uit /etc/inetd.conf halen en dan het proces opnieuw opstarten.

1. **Rogue shel backdoor detection.**

Dit wilt zeggen dat een hacker kan meeluisteren via een shell naar de remote port zonder authenticatie. En zo kan de hacker direct commando’s verzenden via de remote port.

**Oplossing:** Regelmatig controleren of de remote host in gevaar is geweest en als het nodig is kan je deze opnieuw installeren.

1. **UnrealIrcd backdoor detection.**

Dit wilt zeggen dat er een backdoor is in de remote IRC server (is een versie van de unreallrcd). Via deze backdoor kunnen hackers attacks versturen.

**Oplossing:** Je kan deze software opnieuw installeren en dan gebruik maken van encryptie.

1. **Unsupported Unix Operating System.**

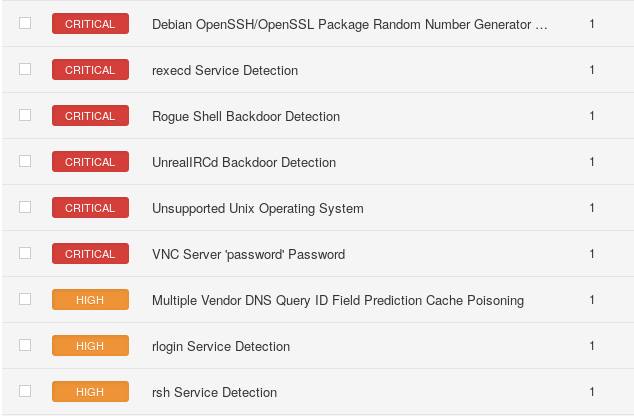
Dit wilt zeggen dan het Operating System niet meer ondersteunt wordt. Hierdoor krijg je ook geen nieuwe security patches.

**Oplossing:** Je Operating System updaten naar een ondersteunde versie.

1. **VNC server “password” password.**

Dit wilt zeggen dat de VNC server beveiligd is met een te zwak wachtwoord. Nessus heeft zich kunnen inloggen met het wachtwoord “password”.

**Oplossing:** Je VNC service beveiligen met een sterk wachtwoord.

****