Bryan Deferm, Greg Blockx, Anthony Heremans

2TinG | 2016-2017

Basic security

Pe opdracht

Inhoud

[Vulnerability Analysis 2](#_Toc482186781)

[Nessus scan op Windows XP met firewall 2](#_Toc482186782)

[Nessus scan op Windows XP zonder firewall 2](#_Toc482186783)

[OpenVas scan Windows XP met firewall 4](#_Toc482186784)

[OpenVas scan Windows XP zonder firewall 4](#_Toc482186785)

[Vergelijking Nessus en OpenVas 4](#_Toc482186786)

[Nessus scan Metasploitable OS (5 vulnerabilities) 5](#_Toc482186787)

[Chatapplicatie 6](#_Toc482186788)

[Infosec Policy 7](#_Toc482186789)

[Basis onderwerpen 7](#_Toc482186790)

[Acceptabel gebruik van de infrastructuur 7](#_Toc482186791)

[Netwerkgebruik 7](#_Toc482186792)

[Printers 7](#_Toc482186793)

[PingPing 8](#_Toc482186794)

[Password policy 9](#_Toc482186795)

# Vulnerability Analysis

## 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.

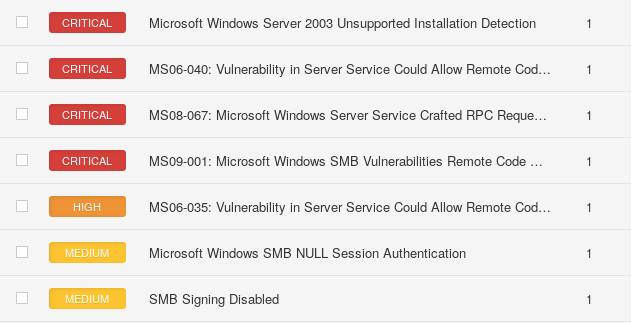
**Oplossing:** Pas de volgende veranderingen toe in het register (regedit):

* 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**

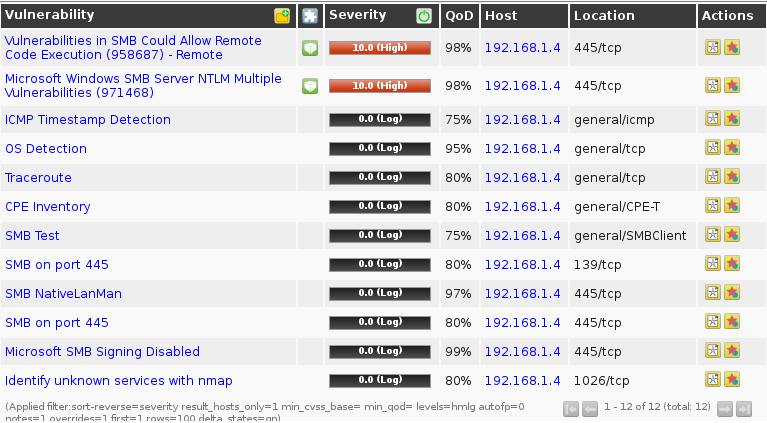
Dit wilt zeggen dat de computer beïnvloed wordt door het ontregelen van het SMB-protocol. Een gevolg hier van kan het overnemen van het systeem of het afwijzen van services zijn.

**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.**

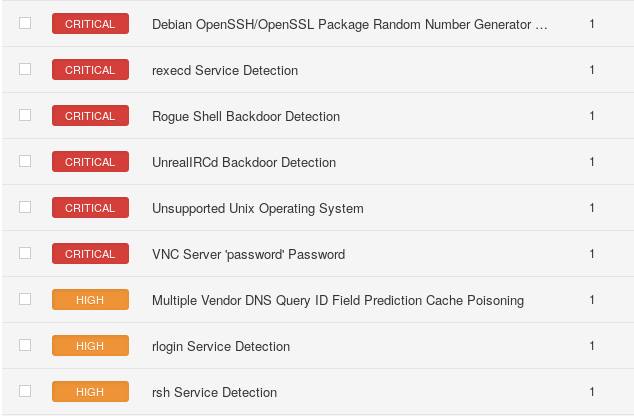
Dit wilt zeggen dan het Operating System niet meer ondersteunt wordt. Hierdoor krijg je ook geen nieuwe security patches.

**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.

****

# Chatapplicatie

Zie .NET gedeelte.

# Infosec Policy

## Basis onderwerpen

### Acceptabel gebruik van de infrastructuur

Het materiaal/infrastructuur van de school mag enkel gebruikt worden voor educatieve doeleinden en mag dus niet worden gebruikt voor illegale of commerciële praktijken.

*Dit is zodat de school niet verantwoordelijk kan worden gesteld voor eventuele illegale activiteiten. Er mag niet illegaals worden gedaan met de apparatuur en deze mag dan ook niet verhuurd/geleend worden voor commerciële doeleinden.*

### Netwerkgebruik

Elke gebruiker mag vrij op het netwerk, zowel met draad als draadloos. Sommige sites worden beperkt door firewall regels, op basis van categorieën.

*Zo kan men sites blokkeren die niet op school thuishoren, zoals pornografische of illegale sites. Maar ook sites die enkel in privé horen toegankelijk te zijn. Zo wordt de kans op malware verlaagd.*

#### Wired

Mac adres en patchpoort worden bijgehouden.

*Zo kan er worden nagekeken wie op welke locatie en op welk tijdstip inlogt. Dit op basis van het mac adres van de netwerkkaart.*

#### Wireless

Mac adres en access point worden bijgehouden.

*Zo kan er worden nagekeken wie op welke locatie en op welk tijdstip inlogt. Dit op basis van het mac adres van de netwerkkaart.*

### Printers

De default waardes zijn zwart-wit en dubbelzijdig afdrukken, maar dit kan worden aangepast.

*Dubbelzijdig printen is beter voor het milieu en voor het werken naar een papiervrije school. Het zwart-wit printen is voor het besparen op duurdere kleurpatronen.*

#### Student :

Betaald met pingping. €0.01/blad voor zwart-wit en €0.10/blad voor kleur.

*Alle documenten die in de les worden gezien, worden doorgegeven als PDF, op deze manier kan de student zelf beslissen welke documenten afgedrukt dienen te worden. Zo gaat men verspilling van papier tegen. Door met de pingping te werken kan er ook worden bijgehouden hoeveel een student print en is het identificeren van de student makkelijker bij het afhalen van de geprinte documenten. De reden van het grote prijsverschil is omdat gekleurde inkt duurder is bij aankoop.*

#### Personeel:

Afdrukken is gratis na vertoon van pingping kaart.

*Het personeel kan gratis printen aangezien het de werkplek is, dit wordt door de school bekostigt. Het gebruik van pingping is zodat het personeelslid kan worden geïdentificeerd en dus gratis kan printen. Zo wordt er ook voor gezorgd dat een student niet de geprinte documenten van een docent kan afhalen. Via deze weg kan er ook worden nagegaan hoeveel een personeelslid print om misbruik tegen te gaan.*

### PingPing

Elke gebruiker krijgt bij de inschrijving een pingping account. Deze wordt zowel voor identificatie als voor betaling gebruikt.

*Zo kan men er zeker van zijn dat de gebruiker altijd een kaart heeft na de inschrijving. Toegang tot bepaalde delen van een gebouw kan door de beheerder gegeven of ontnomen worden. Dit gebeurt door groepsbeheer op basis van functie. Dit zorgt ook voor extra veiligheid bij verlies van deze kaart, de beheerder kan deze dan onmiddellijk blokkeren. Ook de schoolomgeving is hierdoor een stuk veiliger, want men is niet meer verplicht om met cash rond te lopen, aangezien er betaald kan worden met pingping. De betalingen aan het buffet of aan de drankautomaat verlopen hierdoor een pak vlotter en zo kan men ook registreren wat er het meest aangekocht wordt en zich hiervoor aanpassen. Het saldo van een kaart wordt bijgehouden op de server, niet op de kaart.*

Een maximum van €100 per herlading.

*De kaart is niet beveiligd met een code, hierdoor is het gevaarlijk bij diefstal. Daarom wordt er een maximumbedrag aangeraden. €100 is hierbij voldoende, zonder dat je elke week opnieuw moet herladen.*

Herladen kan via de terminals in de gebouwen of op de website met de bankkaart

*De terminals in de gebouwen zorgen voor een groot gebruiksgemak zodat men niet wordt verplicht de laptop te nemen en in te loggen op de site. Het opladen op de site is vooral handig indien je bij je thuis wilt herladen, de avond voor je naar school moet, zodat je de lange rij bij de terminals kan vermijden.*

Het geld kan worden overgeschreven via de site, terug naar de bankrekening.

*Stel dat de persoon teveel geld op de kaart gezet had, dan kan hij het geld altijd terug overzetten en is hij niet verplicht dit te spenderen. Ook bij het sluiten van het account kan het geld nog worden overgeschreven. Indien de persoon in geldnood zit en nog geld op pingping had, kan dit worden teruggestort.*

#### Alle studenten behalve TIN SNB

Pingping kaart mag worden uitgeleend op eigen risico. De kaart kan worden geblokkeerd, hiervoor dient men langs te gaan bij het secretariaat in gebouw D. men kan de kaart ook via de site blokkeren.

*Aangezien de kaart enkel gebruikt wordt om te betalen en om te printen, is het uitlenen hiervan op eigen risico.*

#### Studenten TIN SNB, docenten, IT personeel en management

Kaart mag enkel persoonlijk gebruikt worden en mag niet worden uitgeleend. Bij verlies dient de kaart onmiddellijk gedeactiveerd te worden via de website.

*De kaart wordt niet enkel voor betalingen gebruikt, maar ook om lokalen, kantoren of server rooms binnen te komen. Het uitlenen is dus verboden.*

Een nieuwe kaart kan worden aangevraagd voor €8, het bedrag wat er nog op stond wordt direct overgezet op de andere kaart, de nieuwe kaart kan na 16u gebruikt worden.

### Password policy

Het paswoord dient minstens 8 tekens lang te zijn en moet minstens 3/4 van de verschillende tekensoorten (caps, no caps, getallen, speciale tekens) bevatten.

*De lengte en sterkte van het paswoord zorgt voor een extra beveiliging zonder het te moeilijk te maken voor de gebruiker.*

Vervallen van paswoord:

* Student : elk jaar
* Docent : elke 6 maanden
* IT dienst : elke 3 maanden

*Als de student éénmaal per jaar moet veranderen, is het makkelijker te onthouden. Docenten en IT dienst moeten vaker veranderen omdat ze via hun account toegang hebben tot gevoelige informatie.*