



**HoGent**

Faculteit Bedrijf en Organisatie

Beveiliging van een Windows Server 2012 R2 webserver met ASP.NET applicatie

Nathan Baele

Scriptie voorgedragen tot het bekomen van de graad van  
Bachelor in de toegepaste informatica

Promotor:  
Bert Van Vreckem  
Co-promotor:  
Selami Top

Instelling: —

Academiejaar: 2014-2015

Tweede examenperiode



Faculteit Bedrijf en Organisatie

Beveiliging van een Windows Server 2012 R2 webserver met ASP.NET applicatie

Nathan Baele

Scriptie voorgedragen tot het bekomen van de graad van  
Bachelor in de toegepaste informatica

Promotor:  
Bert Van Vreckem  
Co-promotor:  
Selami Top

Instelling: —

Academiejaar: 2014-2015

Tweede examenperiode

## **Samenvatting**

Vandaag de dag komt cybercrime meer en meer voor in de bedrijfswereld. Professionele hackers en oplichters proberen binnen te dringen in een netwerk van een bedrijf om gevoelige informatie te gebruiken om zaken te verkrijgen of om het bedrijf op te lichten. Dit probleem groeit even snel als de groei van netwerken in het bedrijfsleven. Daarom is het belangrijk om een zeer goed beveiligd netwerk te hebben tegen bedreigingen van zowel binnen als buiten het bedrijf.

De doelstelling van dit onderzoek is om een duidelijk overzicht te geven van welke beveiligings best practices er zeker aanwezig moeten zijn op een webserver in een netwerk om beschermd te zijn tegen enkele van de bekendste aanvallen. Na het lezen van deze scriptie zou het mogelijk moeten zijn om zelf een beveiligde webserver op te zetten die voorzien is van deze best practices.

Om dit probleem te onderzoeken heb ik op voorhand enkele onderzoeksvragen vastgesteld. Wat zijn de bekendste soorten van externe en interne bedreigingen en hoe worden deze het efficiëntst opgelost? Hoe word de webserver zo optimaal mogelijk beveiligd? Waar kan een administrator aanvallen terugvinden in de logs?

# Voorwoord

Deze scriptie zou niet tot stand gekomen zijn zonder de hulp van mijn stagementor en co-promotor Selami Top. Bij het uittesten en onderzoeken van de onderzoeksvragen werd gebruik gemaakt van het netwerk van Hardo bvba, het bedrijf waar Selami Top zaakvoerder van is. Dit zorgde ervoor dat alle conclusies en antwoorden bedrijfsecht zijn en gaf mij een betere kijk op een realistische beveiliging.

Verder wil ik ook mijn promotor Bert Van Vreckem bedanken die mij enorm heeft geholpen met deze bachelorproef tot stand te brengen. Zijn structurele en inhoudelijke tips brachten deze scriptie naar een hoger niveau. Het delen van zijn kennis zorgde er ook voor dat dit onderzoek een betere kwaliteit heeft.

Mijn ouders Johan Baele en Kathleen van Wassenhove zijn ook een grote hulp geweest. Deze hebben mij enorm gesteund tijdens het onderzoeken van dit onderwerp en hebben mij geholpen met het nalezen van de eindtekst en het verbeteren van enkele taal -en layoutfouten.

Tot slot wil ik alle auteurs bedanken van de boeken, websites, handleidingen, videolessen, ... die ik heb gelezen. Dankzij hun bijdrage is de kwaliteit van deze scriptie en mijn kennis enorm verbeterd.

# Inhoudsopgave

<b>1</b>	<b>Inleiding</b>	<b>4</b>
1.1	Probleemstelling en Onderzoeksvragen . . . . .	5
1.1.1	Zijn de best practices voldoende als beveiliging tegen een externe of interne aanval? . . . . .	5
1.1.2	Wat is de beste manier om als administrator sporen terug te vinden van een aanval? . . . . .	5
<b>2</b>	<b>Methodologie</b>	<b>7</b>
<b>3</b>	<b>Opzetten servers met best practises beveiliging</b>	<b>9</b>
3.1	Installatie + configuratie ADServer . . . . .	9
3.2	Installatie + configuratie WebServer . . . . .	10
3.3	Installatie + configuratie aanvallersmachine . . . . .	11
3.4	Besturingssysteem best practices WebServer . . . . .	11
3.4.1	Wachtwoordbeleid . . . . .	11
3.4.2	Accountbeheer . . . . .	13
3.4.3	Updates . . . . .	13
3.4.4	Backup . . . . .	14
3.4.5	Firewall . . . . .	14
3.4.6	Anti-virus . . . . .	15
3.5	IIS best practices WebServer . . . . .	17
3.5.1	Dedicated server . . . . .	17
3.5.2	Inetpub . . . . .	17
3.5.3	Modules . . . . .	17
3.5.4	Opties methode uitschakelen . . . . .	18
3.5.5	Dynamische IP restricties . . . . .	19
3.5.6	Request Filtering Rules . . . . .	20
3.5.7	Inschakelen logs . . . . .	20
3.6	SQL Server best practices WebServer . . . . .	21
3.6.1	Uitschakelen van onnodige features . . . . .	21

3.6.2	Patchen en updaten . . . . .	21
3.6.3	Loggen van aanmeldpogingen . . . . .	21
<b>4</b>	<b>Risico-analyse</b>	<b>22</b>
4.1	Assets . . . . .	22
4.2	Bedreigingen en risicofactor . . . . .	23
4.2.1	Applicatielaag . . . . .	23
4.2.2	Transportlaag . . . . .	26
4.2.3	Internetlaag . . . . .	27
4.2.4	Netwerkttoeganglaag . . . . .	29
4.3	Prioriteiten . . . . .	30
<b>5</b>	<b>Penetration Testing</b>	<b>31</b>
5.1	Applicatie laag . . . . .	31
5.1.1	Brute force Hydra-aanval . . . . .	31
5.1.2	SQL injection . . . . .	33
5.2	Transportlaag . . . . .	34
5.2.1	Socketstress DDOS-aanval . . . . .	34
5.3	Netwerklaag . . . . .	35
5.3.1	Malware applicaties . . . . .	35
<b>6</b>	<b>Post mortem</b>	<b>37</b>
6.1	Manueel . . . . .	37
6.1.1	RAM-geheugen . . . . .	37
6.1.2	Geblokkeerde accounts . . . . .	37
6.1.3	Malware . . . . .	38
6.2	Automatisch . . . . .	38
6.2.1	Prestatiemeter . . . . .	38
<b>7</b>	<b>Conclusie</b>	<b>40</b>

# Hoofdstuk 1

## Inleiding

„The bad guys are winning”. Met deze woorden in een artikel van Wiener-Bronner (2014) is het duidelijk dat vandaag de dag cybercrime meer en meer voorkomt. Professionele hackers en oplichters proberen binnen te dringen in een netwerk/server van een bedrijf om gevoelige informatie te verkrijgen en te gebruiken om het bedrijf op te lichten. Daarom is het belangrijk om een zeer goed beveiligd netwerk te hebben tegen bedreigingen van zowel binnen als buiten het bedrijf en dat is ook één van de doelstellingen in dit onderzoek.

In deze scriptie zal een fictief netwerk opgezet worden dat een domeincontroller en een webserver zal bevatten. Deze beide virtuele machines zullen geconfigureerd worden volgens de algemene best practices om zo de beveiliging van deze servers te verbeteren. Er zijn natuurlijk honderden verschillende soorten aanvallen en mogelijkheden tot cybercrime of tot het binnendringen van een netwerk. Enkele van de meest voorkomende aanvallen zijn SQL-injectie, exploits (Siddharth, 2006), DDoS, port scans en social engineering (Gibson, 2011), maar er zijn nog immens veel soorten.

Er moet dus ergens een keuze gemaakt worden welke aanvallen er in dit onderzoek zullen besproken worden. Dit zal gebeuren a.d.h.v. een risico-analyse van de webserver om te kijken welke aanvallen het meeste kans hebben om uitgevoerd te worden en dus van belang zijn. De aanvallen die de grootste kans hebben of die het meeste schade kunnen toebrengen aan de webserver zullen dan later in dit onderzoek één voor één besproken worden.

Deze aanvallen zullen dan ook uitgevoerd worden met een Kali Linux-aanvallersmachine tegen de webserver om te kijken of de eerder geïmplementeerde best practices voldoende zijn om de server te beveiligen, of dat er extra maatregelen moeten getroffen



worden. Dit heeft niet alleen als doel om de best practices aan te vullen en te verbeteren, maar ook om de typische aanpak van beveiligingsproblemen waar er enkel wordt gehandeld nadat er iets is gebeurd te vermijden. Het probleem hierbij is dat er niet preventief wordt nagedacht en dat er al een aanval is uitgevoerd voordat er naar een oplossing wordt gezocht. Dit kan resulteren in schade of diefstal binnen het netwerk en zo is het dus belangrijk dat het ad-hoc controleren op fouten niet de meest gebruikte beveiligingsmanier is.

Tot slot wordt er gekeken naar hoe de administrator deze aanvallen kan terugvinden in de logs als ze zijn uitgevoerd of nog bezig zijn. Er kan altijd een aanval door de beveiliging geraken en dan is het belangrijk om snel en goed te reageren. Hoe sneller dat een aanval gesignaleerd wordt, hoe sneller er ook een oplossing kan gevonden worden. Dit is cruciaal om toekomstige aanvallen af te weren want hoe langer een zwakte na een aanval onopgelost blijft, hoe meer risico er is dat er meerdere aanvallen zullen plaatsvinden. Dus het maken van geautomatiseerde logs en scans kan ervoor zorgen dat problemen bijna direct worden opgemerkt.

## **1.1 Probleemstelling en Onderzoeksvragen**

### **1.1.1 Zijn de best practices voldoende als beveiliging tegen een externe of interne aanval?**

Allereerst wordt de webserver geconfigureerd volgende de best practices van Cott (2012), Microsoft (2013), Poley (2013), Posey (2011) en Vialle (2012). Daarna wordt er een risico-analyse uitgevoerd en wordt er gekeken naar welke aanvallen relevant zijn en verder zullen onderzocht worden. Deze selectie van aanvallen zullen uitgevoerd worden om te kijken of de geïmplementeerde best practices voldoende zijn om de server te beveiligen of dat er aanvullingen moeten gedaan worden.

### **1.1.2 Wat is de beste manier om als administrator sporen terug te vinden van een aanval?**

Het spreekt voor zich dat, wanneer er zich een aanval voordoet of heeft voorgedaan, dat een netwerkbeheerder dit direct of toch zo snel mogelijk wilt te weten komen. Als er een aanval gaande is dan is het belangrijk dat de beheerder dit snel weet en dat deze snel de oorzaak vindt en weet wat er precies aan het gebeuren is. Hetzelfde geldt voor wanneer er een aanval heeft plaatsgevonden in de geschiedenis. Het is de taak

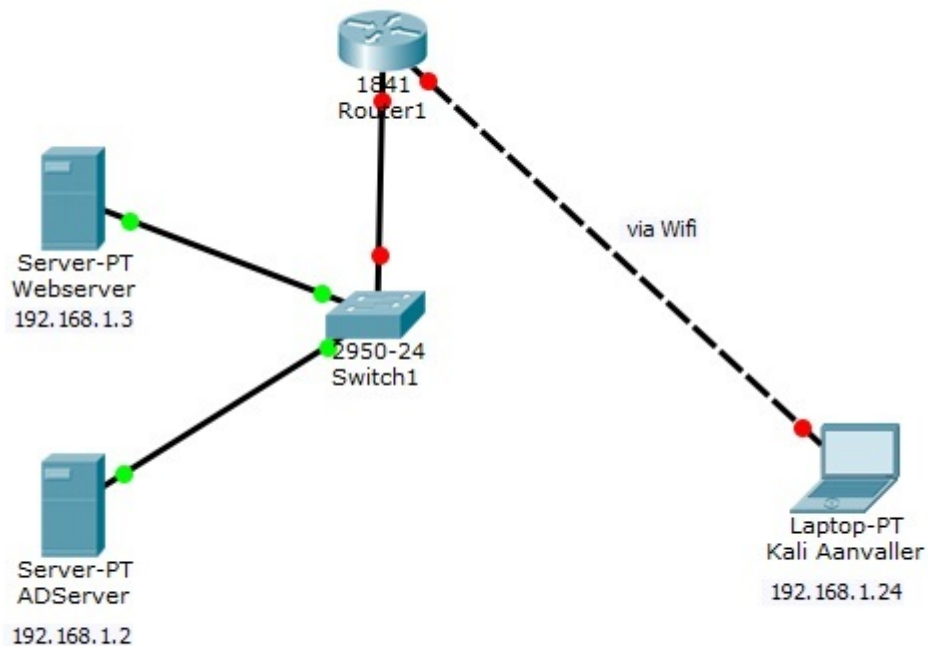
van de administrator om ervoor te zorgen dat aanvallen makkelijk terug te vinden zijn ofwel manueel ofwel automatisch zodat deze tijdig kunnen onderbroken worden of niet meer zullen voorvallen.

# Hoofdstuk 2

## Methodologie

Dit onderzoek bestaat uit de volgende methodiek:

1. Een dergelijke basiskennis is vereist dus het verrichten van onderzoek en lezen van lectuur is een essentiële eerste stap.
2. Opzetten van een goede testomgeving met één Windows Server 2012 R2 domeincontroller, één Windows Server 2012 R2 webserver met ASP.net-applicatie draaiende als slachtoffer en één Kali Linux-machine als aanvaller. De Webserver zal geconfigureerd worden volgens de best practices.
3. Een risicoanalyse uitvoeren en kijken wat de belangrijkste bedreigingen zijn voor dit type systemen.
4. Met behulp van penetration testing tools beveiligingsproblemen zoeken en uitbuiten. Hier wordt er vanuit gegaan dat er geen fysieke toegang is tot de server dus een boot-cd insteken, rebooten en het administrator wachtwoord wijzigen zal niet lukken. Er wordt een lijst gemaakt met welke aanvallen er gaan gedaan worden en welke succesvol worden uitgevoerd en welke falen. Indien een aanval succesvol wordt uitgevoerd, dan zullen de best practices moeten aangevuld worden.
5. Het uitvoeren van een post-mortem om sporen van inbraak bloot te leggen en kijken waar het probleem zich bevindt.



Figuur 2.1: Proefopstelling

In figuur 2.1 is te zien welke machines allemaal nodig zijn om dit onderzoek tot een goed einde te brengen. Ten eerste is er een Active Directory-server nodig die ook domeincontroller is in het domein en deze server is ook nog DNS-server ook. Dan is er de webserver die lid is van hetzelfde domein als de ADServer natuurlijk. Deze zijn aangesloten aan een switch en een router. Ten slotte is er ook nog een aanvallersmachine om te proberen de server te hacken. Deze is ook aangesloten aan een router op een andere locatie. Tot slot wordt er gebruik gemaakt van VMWare Workstation om al deze virtuele machines te maken met elkaar te verbinden.

## Hoofdstuk 3

# Opzetten servers met best practises beveiliging

### 3.1 Installatie + configuratie ADServer

De Windows Server 2012 R2-virtuele machine genaamd „ADServer” is de eerste die moet worden opgezet. In VMWare Workstation wordt er 60GB geheugen gealloceerd voor deze virtuele machine samen met één netwerkadapter en 2GB aan RAM-geheugen. Nadat Windows Server 2012 R2 is geïnstalleerd op deze virtuele machine, krijgt deze de naam „ADServer” en wordt deze heropgestart. Daarna kan er begonnen worden met het installeren van de nodige rollen. De eerste rol die wordt geïnstalleerd is de rol textitActive Directory Domain Services. Daarna wordt de ADServer opgewaardeerd naar domeincontroller in het fictieve domein „Baele.be”. Op de server is één netwerkadapters aanwezig en deze wordt handmatig ingesteld. De server krijgt als IP-adres 192.168.1.2 mee, als subnetmask 255.255.255.0, als default gateway 192.168.1.2 en als DNS-server 127.0.0.1.

Het volgende dat moet gebeuren is het installeren en configureren van de DNS-rol. Dit is vrij simpel en neemt niet veel tijd in beslag. In het scherm „DNS-beheer” wordt er in het tabblad „Zones voor reverse lookup” een zone aangemaakt met de naam „1.168.192.in-addr.arpa” en daarna wordt er een PTR-record aangemaakt die verwijst naar de net geconfigureerde LANadapter met het juiste IP-adres. Hierna wordt de DHCP-rol geïnstalleerd en wordt er een nieuwe scope aangemaakt met de naam „TestScope”. Het eerste IP-adres in het bereik is 192.168.1.1 en het laatste 192.168.1.254. De adressen van 192.168.1.1 tot 192.168.1.20 worden uitgesloten voor distributie. De WebServer wordt de router dus het IP-adres dat hier wordt

meegegeven is 192.168.1.3. Dit is het IP-adres die later aan de router/WebServer wordt gegeven.

## **3.2 Installatie + configuratie WebServer**

De installatie start op dezelfde manier als de voorgaande machine, maar in dit geval wordt de machine *WebServer* genoemd en zijn er twee netwerkadapters aanwezig, één die is verbonden met het internet (Internetadapter) en een andere die is verbonden met het LAN (LANadapter). De internetadapter staat geconfigureerd als NAT en de IP -en DNS-informatie worden alletwee automatisch aangewezen. Bij de LANadapter zijn de instellingen anders, hier staat deze configureerd als *Custom: specific virtual network* en wordt er gekozen om het virtuele network de naam *VMnet0* mee te geven. Hierdoor moeten de IP -en DNS-instellingen handmatig geconfigureerd worden. De server krijgt al IP-adres 192.168.1.2 mee, als subnetmask 255.255.255.0, als default gateway 192.168.1.2 en als DNS-server 127.0.0.1.

Deze server wordt ook lid gemaakt van het domein *Baele.be*. Verder wordt er ook de rol *Externe Toegang* toegevoegd. Deze stellen we zo in dat de netwerkadapter waar het internet van komt wordt gebruikt voor andere hosts die verbonden zijn met het netwerk en die op het internet moeten. De WebServer wordt dus zo een router.

Op deze server is het belangrijk dat de rol *Internet Information Service 8* (IIS8) is geïnstalleerd. Deze is al automatisch geïnstalleerd bij het installeren van de rol *Externe Toegang*. Verder is de installatie van databanksoftware ook nodig. In dit geval wordt er gebruik gemaakt van Microsoft SQL Management Studio 2014. Bij de installatie is het aangeraden om *Use Microsoft Update to check for updates* aan te vinken. Na de installatie wordt er een testdatabase aangemaakt met de naam *TestDatabase* en in deze database wordt er een tabel aangemaakt met de naam *People* met de rijen *PeopleID*, *Fname*, *Lname* en steek twee willekeurige waarden in deze tabel. Tot slot wordt er nog een nieuwe stored procedure aangemaakt met de volgende inhoud:

```
Create Procedure Test_GetPeople
AS
Select * from People;
```

De volgende stap is om een basis ASP.net-applicatie te maken en dit wordt gedaan met de hulp van Nuckolls (2011). Met behulp van deze persoon zijn tutorial, de link is te vinden in de bibliografie, is er direct een ASP.net-applicatie met een achterliggende

database toegevoegd.

### 3.3 Installatie + configuratie aanvallersmachine

De derde en laatste virtuele machine die nodig is in dit onderzoek is de Kali Linux-aanvallersmachine. Deze is vrij makkelijk te installeren en heeft ook niet zo hoge systeemvereisten. Voor deze machine is er maar 20Gb aan gealloceerd geheugen nodig samen met 1 netwerkadapter die op *VMnet0* staat en 512MB aan RAM-geheugen. Bij het starten van de installatie moet er gekozen worden voor *graphical install*. De meeste stappen zijn voor de hand liggend, maar bij partition disks wordt er *guided-use entire disk* het best geselecteerd. De naam van de machine wordt ingesteld op *KaliAanvaller*. Op het moment dat er wordt gevraagd van welk netwerk deze computer deel uit maakt, wordt er *baele.be* gekozen. Voor de rest zijn de overige stappen niet zo belangrijk en is de installatie zo afgerond.

### 3.4 Besturingssysteem best practices WebServer

Nu dat de webserver is geïnstalleerd, kan er begonnen worden aan het toepassen van de best practices. Het is zeer belangrijk dat dit eerst wordt gedaan voordat de server wordt opgenomen in het netwerk. In dit deel worden alle best practices van het besturingssysteem besproken van een sterk wachtwoordbeleid tot het regelmatig updaten van de server.

#### 3.4.1 Wachtwoordbeleid

##### Wachtwoord geschiedenis afdwingen

Dit is een policy die ervoor zorgt dat gebruikers, als ze van wachtwoord moeten veranderen, ze niet kunnen wisselen tussen altijd dezelfde wachtwoorden. Er kunnen in totaal tot wel 24 wachtwoorden opgeslaan worden in de wachtwoordgeschiedenis dus zo is de kans klein dat gebruikers blijven wisselen tussen dezelfde wachtwoorden. Als een gebruiker slim is kan hij zijn wachtwoord gewoon 24 keer na elkaar wijzigen om dan terug zijn oude antwoord te gebruiken. Dit kan ook voorkomen worden door een *Minimum Password Age Policy* in te stellen zodat een wachtwoord bijvoorbeeld

maar om de 2 dagen kan veranderd worden. (Stanek, 2009)

Dit kan geïmplementeerd worden door naar het *Lokaal beveiligingsbeleid* te gaan en daar te klikken op het *Wachtwoordbeleid*. Er is te zien dat de *Minimale wachtwoord-duur* default staat ingesteld als 1 dag en de wachtwoordgeschiedenis op 24 wachtwoorden dus dit mag zo gelaten worden als best practice.

#### **Wachtwoord regelmatig wijzigen**

Een andere best practice is om het wachtwoord regelmatig eens te veranderen. Dit kan mondeling gebeuren, maar het meest efficiënte is om dit ook te doen a.d.h.v. een policy. Er kan terug gegaan worden naar de voorgaande locatie en daar kan er gekozen worden voor *Maximale wachtwoordduur*. Deze staat default op 42 dagen dit is een goede waarde voor netwerken waar beveiliging zeer belangrijk is want daar wordt er meestal gekozen voor een waarde tussen de 30-90 dagen. Bij netwerken waar de beveiliging niet zo belangrijk is kan dit eerder 120-180 dagen zijn. (Stanek, 2009)

#### **Minimale wachtwoordlengte**

Deze policy, die ook te vinden is op dezelfde plek als de vorige policies, zorgt ervoor dat een gebruiker zijn wachtwoord minimaal een bepaalde lengte moet hebben. Dit heeft als bedoeling om het brute force kraken van wachtwoorden moeilijker tot onmogelijk te maken. Default staat deze policy op 7 dagen maar Stanek (2009) raadt aan om deze policy in te stellen op een lengte van minstens 14 tekens. Dit heeft als reden dat een wachtwoord van 7-8 tekens vandaag de dag op een korte tijd wordt gekraakt door het toepassen van brute force wachtwoord kraken met moderne hardware.

#### **Complexiteit van het wachtwoord**

Het spreekt voor zich dat een wachtwoord zoals *123456* niet acceptabel is. Daarom is het belangrijk dat er een policy is die de complexiteit van een wachtwoord verzekerd. Dit kan alweer gevonden worden op voorgaande locatie waar de policy *Wachtwoorden moeten voldoen aan complexiteitsvereisten* kan worden ingeschakeld. Dit zorgt ervoor dat de wachtwoorden minstens 6 tekens moeten hebben, er kunnen geen gebruikersnamen of gewone namen in voorkomen en wachtwoorden moeten minstens 3 van de 4 verschillende soorten karakters bevatten (normale letters, hoofdletters, nummers en symbolen). (Stanek, 2009)



### 3.4.2 Accountbeheer

#### Uitschakelen van Administrator-account

Eén van de eerste zaken dat moet gebeuren is het uitschakelen van de inlognaam *Administrator*. Dit heeft als reden dat elke persoon weet dat het default account deze naam heeft en zo is het voor hackers gemakkelijker om binnen te breken als deze al de naam van een account met administrator rechten bezitten. Dit account kan uitgeschakeld worden door op de ADServer naar de *Active Directory - gebruikers en computers* te gaan en daar bij *Users* en daar te rechterklikken op het account *Administrator* en deze dan uit te schakelen.

#### Aanmaken eigen administrator-account

Nadat in de vorige stap het default administrator-account is uitgeschakeld, moet er natuurlijk weer een nieuw account komen zodat er toch nog administrator-taken kunnen uitgevoerd worden. Dit kan gedaan worden door op dezelfde locatie als de voorgaande stap een nieuwe gebruiker toe te voegen, in dit geval met de naam *BaeleAdministrator*, en deze lid te maken van de groepen *Administrators*, *Domeinadministrators* en *domeincontrollers*. Nu is het best om even uit te loggen en terug in te loggen met het nieuwe account.

### 3.4.3 Updates

Nog een belangrijke onderdeel van een server met best practice beveiliging, is het regelmatig downloaden en installeren van updates. Bij het vinden van een nieuw zwak punt of exploit in software, wordt dit al binnen enkele uren op het internet geplaatst en wordt er dus ook gewerkt aan een oplossing. Als de server en applicaties continue worden geupdate, dan is de kans veel kleiner dat er een exploit zal uitgebuit worden. (Cott, 2012). Automatische updates worden echter zo goed als nooit gedaan. De voorgestelde updates worden best door de administrator gedownload en uitgetest in een virtuele testomgeving zodat er zekerheid is dat deze update geen problemen met zich meebrengt. Nadat deze test is geslaagd, kan de update op de webserver geïnstalleerd worden.

### **3.4.4 Backup**

Het maken van geautomatiseerde backups is essentieel voor een server binnen een netwerk. Een fout, probleem of aanval kan elke moment van de dag gebeuren en als dit gebeurt moet het mogelijk zijn om het systeem terug te zetten van een eerder gemaakte backup. In de Windows Server Backup-wizard kan dit worden ingesteld voor elke harde schijf. In dit geval wordt er enkel elke nacht om 03:00u een back-up genomen van de C-schijf, maar dit varieert van bedrijf tot bedrijf en hangt af van hoeveel geheugen er beschikbaar is voor back-ups en welke dataschijven het belangrijkste zijn.

### **3.4.5 Firewall**

De firewall is enorm belangrijk en heeft vooraf al een configuratie meegekregen. Er is echter één aanpassing van de configuratie die in de praktijk veel wordt toegepast en die ook door Nabors (2013) wordt genoemd als een best practise-instelling voor een Firewall-configuratie. Dit betreft het blokkeren van alle uitgaande verbindingen die niet overeenkomen met één van de gedefinieerde regels.

Dit wordt gedaan door naar de eigenschappen te gaan en daar in alledrie de profielen de uitgaande verbindingen op „blokkeren” te zetten. Standaard staat dit geconfigureerd als „toestaan”. Hierna kunnen er eigen inkomende en uitgaande regels geconfigureerd worden naargelang de applicaties die op de server komen te staan en welke poorten open of dicht moeten zijn. Bij uitgaande verbindingen is het belangrijk dat de TCP-poorten 80 (http) en 443 (https) worden toegevoegd aan de uitzonderingen. Nadat deze poorten zijn toegevoegd dan ziet de verzameling van toegestane uitgaande verbindingen eruit als in figuur 3.1 te zien is.

## HOOFDSTUK 3. OPZETTEN SERVERS MET BEST PRACTISES BEVEILIGING

Naam	Groep	Profiel	Ingeschakeld	Bewerking	Overschrijven	Programma	Lokaal adres	Extern adres	Protocol	Lokale poort	Externe poort
Core Networking - Aanvraag voor neigh...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	ICMPv6	Willekeurig	Willekeurig
Core Networking - Advertisement voor n...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	ICMPv6	Willekeurig	Willekeurig
Core Networking - Dynamic Host Config...	Core Networking	Alle	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	UDP	68	67
Core Networking - Dynamic Host Config...	Core Networking	Alle	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	UDP	546	547
Core Networking - Groepsbeleid (NP-Out)	Core Networking	Domein	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	TCP	Willekeurig	445
Core Networking - Groepsbeleid (TCP-Out)	Core Networking	Domein	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	TCP	Willekeurig	Willekeurig
Core Networking - Internet Group Mana...	Core Networking	Alle	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	IGMP	Willekeurig	Willekeurig
Core Networking - IPHTTPS (TCP-Out)	Core Networking	Alle	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	TCP	Willekeurig	IPHTTPS
Core Networking - IPv6 (IPv6-Out)	Core Networking	Alle	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	IPv6	Willekeurig	Willekeurig
Core Networking - Multicastlijstener gere...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Lokaal subnet	ICMPv6	Willekeurig	Willekeurig
Core Networking - Pakket te groot (ICMP...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	ICMPv6	Willekeurig	Willekeurig
Core Networking - Parameterprobleem (I...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	ICMPv6	Willekeurig	Willekeurig
Core Networking - Query voor multicast...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Lokaal subnet	ICMPv6	Willekeurig	Willekeurig
Core Networking - Rapport voor multica...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Lokaal subnet	ICMPv6	Willekeurig	Willekeurig
Core Networking - Rapport voor multica...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Lokaal subnet	ICMPv6	Willekeurig	Willekeurig
Core Networking - Routeraanvraag (ICM...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Lokaal subn...	ICMPv6	Willekeurig	Willekeurig
Core Networking - Router-advertisement...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	fe80::/64	Lokaal subn...	ICMPv6	Willekeurig	Willekeurig
Core Networking - Teredo (UDP-Out)	Core Networking	Alle	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	UDP	Willekeurig	Willekeurig
Core Networking - Tijd overschreden (IC...	Core Networking	Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	ICMPv6	Willekeurig	Willekeurig
DHCPv4 Relay-agent (Client) (UDP-Out)	DHCP Relay-agent	Alle	Ja	Toestaan	Nee	%systemroo...	Willekeurig	Willekeurig	UDP	67	Willekeurig
DHCPv6 Relay-agent (Server) (UDP-Out)	DHCPv6 Relay-agent	Alle	Ja	Toestaan	Nee	%systemroo...	Willekeurig	Willekeurig	UDP	547	Willekeurig
FTP-server (FTP Traffic-Out)	FTP-server	Alle	Ja	Toestaan	Nee	%windir%\s...	Willekeurig	Willekeurig	TCP	20	Willekeurig
FTP-server, beveiligd (FTP SSL Traffic-Out)	FTP-server	Alle	Ja	Toestaan	Nee	%windir%\s...	Willekeurig	Willekeurig	TCP	989	Willekeurig
HTTP (80)		Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	TCP	Willekeurig	80
HTTPS (443)		Alle	Ja	Toestaan	Nee	Willekeurig	Willekeurig	Willekeurig	TCP	Willekeurig	443
Netwerk - DNS (UDP-Out)	Core Networking	Alle	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	UDP	Willekeurig	53
Netwerk - groepsbeleid (LSASS-Out)	Core Networking	Domein	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Willekeurig	TCP	Willekeurig	Willekeurig
Netwerk detecteren (LLMNR-UDP-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Lokaal subnet	UDP	Willekeurig	5355
Netwerk detecteren (NB-Datagram-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	UDP	Willekeurig	138
Netwerk detecteren (NB-Name-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	UDP	Willekeurig	137
Netwerk detecteren (Pub WSD-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Lokaal subnet	UDP	Willekeurig	3702
Netwerk detecteren (SSDP-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Lokaal subnet	UDP	Willekeurig	1900
Netwerk detecteren (UPnPHost-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Lokaal subnet	TCP	Willekeurig	2869
Netwerk detecteren (UPnP-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	TCP	Willekeurig	2869
Netwerk detecteren (WSD Events-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	TCP	Willekeurig	5357
Netwerk detecteren (WSD EventsSecure...	Netwerk detecteren	Privé	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	TCP	Willekeurig	5358
Netwerk detecteren (WSD-Out)	Netwerk detecteren	Privé	Ja	Toestaan	Nee	%SystemRo...	Willekeurig	Lokaal subnet	UDP	Willekeurig	3702
Routering en RAS (GRE-Out)	Routering en RAS	Alle	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	GRE	Willekeurig	Willekeurig
Routering en RAS (L2TP-Out)	Routering en RAS	Alle	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	UDP	Willekeurig	1701
Routering en RAS (PPTP-Out)	Routering en RAS	Alle	Ja	Toestaan	Nee	System	Willekeurig	Willekeurig	TCP	Willekeurig	1723
Uitgaand TCP-verkeer voor Message Que...	Message Queueing	Alle	Ja	Toestaan	Nee	%systemroo...	Willekeurig	Willekeurig	TCP	Willekeurig	Willekeurig
Uitgaand UDP-verkeer voor Message Que...	Message Queueing	Alle	Ja	Toestaan	Nee	%systemroo...	Willekeurig	Willekeurig	UDP	Willekeurig	Willekeurig

Figuur 3.1: Alle toegestane uitgaande verbindingen

### 3.4.6 Anti-virus

#### Goede anti-virus installeren

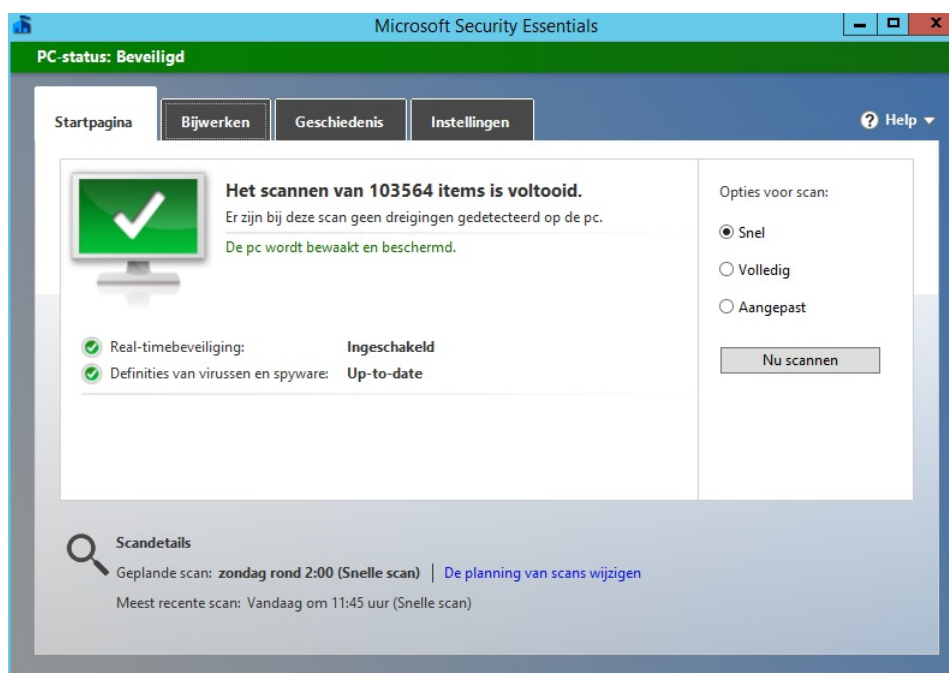
Een degelijke anti-virus is enorm belangrijk om een server, computer of ander online apparaat te beschermen. Bij het gebruiken van een desktop of laptop voor persoonlijk gebruik, is een gratis versie van een bepaalde anti-virus-software voldoende. Voor in een bedrijfsomgeving is het beter dat er een betaalde versie wordt genomen aangezien deze veel meer functies en opties hebben. Microsoft heeft een gratis beveiligingssoftware-pakket genaamd *Microsoft Security Essentials*, maar deze heeft geen versie voor op de Windows Server 2012-besturingssystemen te worden geïnstalleerd. Dit wil niet zeggen dat de installatie van deze software niet lukt natuurlijk op een Windows server.

Allereerst moet er gegaan worden naar de website van Microsoft Security Essentials om daar de recentste versie te downloaden en dit voor een Windows 7 64-bit machine. Als deze installer is gedownload dan moet er gegaan worden naar de eigenschappen om daar de compatibiliteit te veranderen naar Windows 7. Hierna moet er een opdrachtprompt

gestart worden en moet er genavigeerd worden naar de map waar de installer is in geplaatst. Daar wordt er met het volgende lijntje

```
mseinstall /disableoslimit
```

de installer succesvol gestart. Bij de installatie hoeft er enkel op *volgende* gedrukt te worden en de software wordt succesvol geïnstalleerd. Hierna kan er een eerste scan worden gestart die de hele server onderzoekt op virussen en spyware nadat deze zichzelf heeft bijgewerkt met de nieuwste updates. (Herring, 2014)



Figuur 3.2: Voorbeeld van succesvolle scan met volgende geplande scan

#### Regelmatig scannen en updaten

Het spreekt voor zich dat deze anti-virus regelmatig moet ge-update worden zodat wanneer er een nieuwe bedreiging gesignaleerd wordt, deze direct kan toegevoegd worden aan de anti-virus software. Door het dagelijks uitvoeren van updates en een anti-virusscan blijft de server optimaal beschermt. Het beste is om dit 's nachts te doen als het netwerk niet gebruikt wordt om zo de gebruikers van het netwerk niet te belasten.

## **3.5 IIS best practices WebServer**

### **3.5.1 Dedicated server**


Het is zeer belangrijk dat IIS een dedicated server is. Het is volgens Microsoft (2013) gebruikelijk om de webserver apart van de domeincontroller te doen. Dit heeft als reden dat er geen lokale accounts zijn op een domeincontroller en deze lokale accounts zijn belangrijk voor een veilige IIS-server. Het samenplaatsen van een DC en een webserver beperkt de beveiligingsmogelijkheden enorm. Bijvoorbeeld een nieuwe exploit die door een hacker wordt gebruikt zal zo niet alleen de webserver aantasten, maar ook het hele netwerk. Daarom zijn deze twee dus het best gescheiden, zoals in deze opstelling het geval is.

### **3.5.2 Inetpub**

De inetpub-map wordt bij elke installatie van IIS aangemaakt en standaard wordt die geplaatst op de C-schijf. Aangezien dit dezelfde schijf is waar het besturingssysteem opstaat, is het gebruikelijk om deze map op een aparte schijf te zetten zodat de toegang tot deze schijf beter kan beschermt worden. De schijf waar het besturingssysteem opstaat kan nooit zo goed beschermt worden als een aparte schijf. (Darmanin, 2014)

### **3.5.3 Modules**

In totaal bevat IIS meer dan 30 modules en deze moeten niet allemaal actief zijn. In de IIS manager kan er in het modulescherm van de geselecteerde website bepaalde modules op inactief gezet worden. In de lijst moet er beslist worden welke modules nodig zijn en de welke overbodig zijn. De overbodige modules kunnen dan worden uitgeschakeld door deze uit de lijst te verwijderen. In dit geval blijven alle modules staan want deze zijn nodig voor het uitvoeren van de applicatie. (Darmanin, 2014) (Microsoft, 2013)

 **Modules**

Gebruik deze functie om systeemeigen en beheerde codemodules te configureren waarmee aanvragen voor de webserver worden verwerkt.

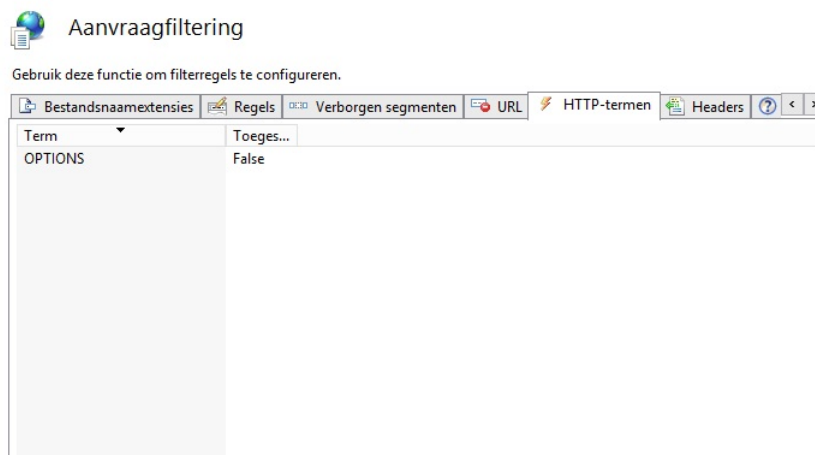
Groeperen op: Geen groepering

Naam	Code	Type module	Type vermelding
AnonymousAuthenticationMo...	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
BasicAuthenticationModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
CertificateMappingAuthentica...	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
CustomErrorModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
CustomLoggingModule	%windir%\System32\inetsrv\l...	Systeemeigen	Lokaal
DefaultDocumentModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
DigestAuthenticationModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
DirectoryListingModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
DynamicCompressionModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
DynamicIpRestrictionModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Systeemeigen	Lokaal
HttpCacheModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
HttpLoggingModule	%windir%\System32\inetsrv\l...	Systeemeigen	Lokaal
HttpRedirectionModule	%windir%\System32\inetsrv\l...	Systeemeigen	Lokaal
IISCertificateMappingAuthenti...	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
IpRestrictionModule	%windir%\System32\inetsrv\i...	Systeemeigen	Lokaal
ProtocolSupportModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
RequestFilteringModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
StaticCompressionModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
StaticFileModule	%windir%\System32\inetsrv\s...	Systeemeigen	Lokaal
UrlAuthorizationModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
WebDAVModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal
WindowsAuthenticationModule	%windir%\System32\inetsrv\...	Systeemeigen	Lokaal

Figuur 3.3: Alle modules die geactiveerd blijven

### 3.5.4 Opties methode uitschakelen

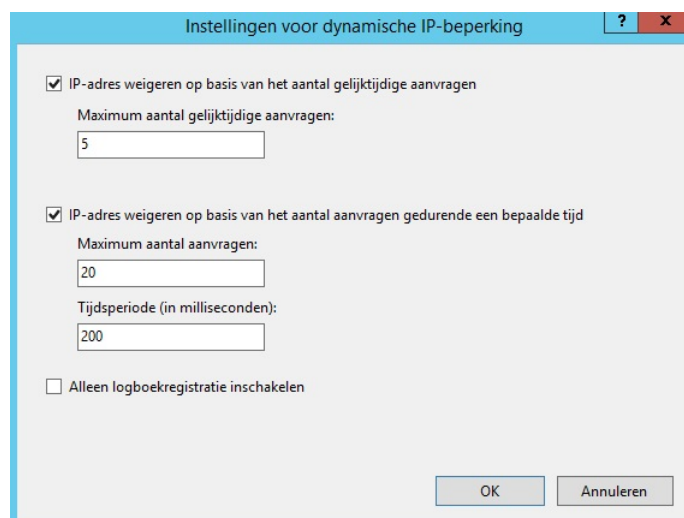
De opties methode geeft een lijst van methodes weer die worden ondersteund door de webserver. Dit kan waardevolle informatie opleveren voor een hacker. Het is dan ook een best practice om deze methode uit te schakelen en dit gebeurt door het woord *OPTIONS* uit te sluiten van de *HTTP Verb request filtering rules* in IIS. Dit wordt gedaan door de website te selecteren in de IIS-manager en dan dubbel te klikken op *aanvraagfiltering* en naar het tabblad *HTTP-termen* te gaan. Hier wordt als actie gekozen *Term weigeren...* en wordt *OPTIONS* ingevuld en op OK gedrukt. Nu staat deze regel als enige in de lijst en is deze best practice in orde gebracht zoals in figuur 3.4 te zien is. (Darmanin, 2014)



Figuur 3.4: De term OPTIONS wordt niet toegestaan

### 3.5.5 Dynamische IP restricties

Het inschakelen van dynamic IP restrictions module zorgt ervoor dat IP-adressen die een bepaald aantal requests hebben verzonden worden geblokkeerd. Hierdoor worden *Denial of Service-aanvallen* voorkomen. Deze module inspecteert het IP-adres van elke request en zal deze requests filteren om de IP-adressen met slechte bedoelingen tijdelijk te blokkeren. Dit kan gedaan worden door naar de IIS-manager te gaan en de naam van de website te selecteren en te dubbelklikken op *beperkingen voor IP-adressen en domeinen*. In het actie paneel wordt er geklikt op *instellingen voor dynamische beperking bewerken..* en kunnen er restricties ingevoerd worden. De eerste twee vakjes van de drie moeten worden aangevinkt en de waarden kunnen naar keuze ingevuld worden, in dit geval is 5-20-200 ingevuld. (Darmanin, 2014)



Figuur 3.5: Instellingen voor dynamische IP-beperking

### 3.5.6 Request Filtering Rules

Het is altijd een goed idee om de verschillende types van HTTP-request die worden verwerkt door IIS te beperken. Door het instellen van uitsluitingen en regels kunnen potentieel gevaarlijke request er nooit doorkomen. Dit gebeurt in de IIS Manager waar de juiste website wordt gekozen en waarna er dubbel wordt geklikt op *Requestfilters*. Hier wordt er gegaan naar het tabblad *regels* en kunnen verschillende filterregels toegevoegd worden. (Darmanin, 2014) (Microsoft, 2013)

### 3.5.7 Inschakelen logs

Door het in te schakelen van het IIS logsysteem worden verschillende HTTP-request gelogged. Indien er problemen voordoen dan kan er hier gekeken worden om een betere kennis te vergaren over het probleem. Dit kan vrij snel en simpel ingeschakeld worden door te gaan naar de IIS manager en daar de gewenste website te selecteren en op *logging* te klikken. Best wordt er gekozen om een nieuw bestand aan te maken want deze bestanden groeien vrij snel. (Darmanin, 2014) (Microsoft, 2013)



## 3.6 SQL Server best practices WebServer

### 3.6.1 Uitschakelen van onnodige features

Nadat de software is geïnstalleerd wordt er best gegaan naar de *SQL Server Configuration Manager Tool* om alle onnodige features te verwijderen. In dit geval zijn er geen extra features geïnstalleerd die niet gebruikt zijn dus hier is dit overbodig. (Maman, 2013)

### 3.6.2 Patchen en updates

Zoals elk Microsoft-product wordt ook SQL Server regelmatig voorzien van de nieuwste updates en patches om de applicatie zo goed mogelijk te beveiligen tegen hedendaagse aanvallen. Het is best dat deze updates eerst eens worden gedownload en geïnstalleerd in een testomgeving om daarna deze in de echte omgeving te implementeren. Dit kan voorkomen dat er bugs in de patch de server in gevaar brengen. (Maman, 2013)

### 3.6.3 Loggen van aanmeldpogingen

Het kan zeer handig zijn om logbestanden bij te houden van iedereen die zich aanmeldt op de SQL Server. Zowel de gelukte als de mislukte login-pogingen zouden moeten geregistreerd worden. Dit kan gedaan worden door naar *SQL Server Management Studio* te gaan en te rechterklikken op de gewenste SQL Server en dan de *Eigenschappen* te selecteren. Aan de linkerkant is er dan de mogelijkheid om op *Security* te klikken en daar kan er gekozen worden voor *Both failed and successful logins*. Als dit is gedaan dan hoeft SQL enkel opnieuw worden opgestart en dan zal dit vanaf nu altijd gebeuren. (Maman, 2013)

# Hoofdstuk 4

## Risico-analyse

Het uitvoeren van een risico-analyse kan in verschillende stappen onderverdeeld worden. Allereerst moet er een opsomming zijn van alles *assets* die zullen onderzocht worden in de risico-analyse. Dan kan er gebrainstormed worden om te kijken welke soort bedreigingen er voor de specifieke server zijn, in dit geval een webserver. Tot slot wordt er m.b.v. enkele tools en wat opzoekwerk gekeken naar welk van deze bedreigingen het belangrijkste zijn. Dit wil zeggen dat er wordt gekeken naar de kans dat deze voorvalt en de mogelijke schade die deze kan toebrengen en zo worden de bedreigingen dan gecatalogiseerd op het vlak van belang.

### 4.1 Assets

In dit geval wordt er gewerkt met een webserver waarop de recentste versie van Windows Server 2012 R2 staat geïnstalleerd met de volgende rollen/programma's/besturingssystemen op geïnstalleerd:

- Windows Server 2012 R2 (waarde 10)
- Internet Information Services 8 (waarde 8)
- Externe toegang, routing (waarde 9)
- Microsoft SQL Server Express 2014 (waarde 7)

De waarde die aan deze assets wordt meegegeven, wordt verklaard in het volgende deel.

## 4.2 Bedreigingen en risicofactor

De soorten bedreigingen kunnen ingedeeld worden per laag van het TCP/IP-model. Hierdoor kan er structureel gekeken worden naar elke laag om zo te kijken welke bedreigingen er aanwezig zijn voordat er wordt verder gekeken. Deze werkwijze zorgt er ook voor dat er minder snel een bedreiging over het hoofd wordt gezien. Er wordt ook gekeken naar wat de mogelijkheid is dat deze aanvallen op een webserver zullen plaatsvinden en wat de mogelijke schade kan zijn en zo wordt er een cijfer meegegeven aan een aanval om te kijken hoe belangrijk deze is. Hoe hoger cijfer, hoe belangrijker het is om de server te beschermen tegen deze aanval. Het berekenen van dit cijfer gebeurt door deze formule: „schade van de aanval x kans op een aanval”. Beide factoren krijgen een cijfer van 1 tot 10 mee waar 10 de hoogste factor (meeste schade of grootste kans op een aanval) voorstelt en 1 dus het omgekeerde. (Sima, 2005)

### 4.2.1 Applicatielaag

Dit is de 4de en de hoogste laag van het TCP/IP-model en is een samenvoeging van de applicatie -, presentatie -en sessielaag van het OSI-model. Deze laag bevat al de "high-level" protocollen zoals DNS, HTTP, Telnet, SSH, FTP, TFTP, SNMP, ... noem maar op. Deze laag heeft ook een rechtstreekse verbinding met de eindgebruiker en de applicaties. (Thomas, 2013)

#### Laag 7 DoS-aanvallen

Een DoS-aanval (of Denial of Service-aanval) die zich afspeelt in de applicatielaag kan een hele server doen crashen. Dit kan gedaan worden door één gebruiker. Indien er meerdere personen samenwerken om een netwerk/server plat te leggen dan wordt er gesproken van een DDoS-aanval (of Distributed Denial of Service-aanval). Een voordeel van DDoS-aanvallen zijn dat deze moeilijker zijn om na te trekken aangezien er verschillende mensen op hetzelfde moment aanvallen i.p.v. één persoon bij een DoS-aanval. (Blagov, 2014) Er zijn verschillende soorten applicatielaag DoS-aanvallen zoals RUDY (R-U-Dead-Yet) waar IIS 8 het slachtoffer wordt en XerXes waar de server via een TCP-connectie het slachtoffer wordt.

De kans dat deze soort aanvallen zullen uitgevoerd worden is zeer groot aangezien het hier gaat over een webserver en die zijn een makkelijk doelwit voor zulke aanvallen. De factor *kans op een aanval* krijgt dus een 9 mee. De schade die een DoS-aanval kan veroorzaken is niet mis, deze kan een server of webapplicatie helemaal offline halen

zolang de aanval duurt. Het spreekt voor zich dat dit vrij irritant is, maar er is geen mogelijkheid tot diefstal van gegevens zoals kredietkaartgegevens of inloggegevens en er kan niets op de server of webapplicatie zelf worden veranderd dus de factor *schade van de aanval* krijgt een 6 mee. Als dan de formule wordt uitgevoerd dan krijgt deze aanval de waarde **54** mee.

### DNS Poisoning

Dit is een aanval die de cache van DNS "vergiftigd" door valse invoer te geven. Zo kan een aanvaller een willekeurige website als facebook of google laten verwijzen naar een IP-adres van zijn eigen website met malware om zo de gebruiker op te lichten. Als een hacker toegang verkrijgt tot een DNS-server en deze valse invoeren plaatst, kan elke persoon binnen een netwerk door het surfen naar een bepaalde website bij een verkeerde website terechtkomen of zelfs bij de machine van de aanvaller zonder dat deze persoon er zelf weet van heeft. Een hacker kan toegang verkrijgen tot een DNS-server door bijvoorbeeld foutjes uit te buiten die in de DNS-software zitten. (Hoffman, 2015)

Op een webserver is de kans dat dit soort aanvallen voorkomen immens klein omdat in de meeste gevallen een DNS-server en een Webserver gescheiden zullen zijn. Zoals eerder besproken is het een best practice om de domeincontroller en de webserver op aparte machines te plaatsen en DNS zit in het merendeel van de gevallen bij de domeincontroller. Hierdoor is krijgt de factor *kans op een aanval* een 1 mee. De schade die deze aanval kan veroorzaken is echter zeer groot. Als een hacker het inlogportaal van een bank namaakt en de gebruiker hier via DNS poisoning naartoe stuurt, kunnen zo bankgegevens gestolen worden en dit kan grote gevolgen hebben. Hierdoor krijgt deze aanval als factor *schade van de aanval* een 9 mee. Dit brengt de totale waarde van de aanval naar de waarde **9**.

### SQL-injectie

Een SQL-injectie is simpel uitgelegd een aanval die slechte code in een webapplicatie gebruikt om hackers SQL-commando's in te geven in een veld om zo toegang te verkrijgen tot een database. Zo kan een hacker bijvoorbeeld bepaalde SQL-commando's ingeven in het login formulier om zo persoonlijke gegevens van anderen te verkrijgen van in de database van de webapplicatie. Bij een succesvolle SQL-injectie kan een hacker niet alleen kijken naar gegevens in een database, hij kan deze gegevens zelfs verwijderen. Dit kan gebeuren bij elk invoerveld waar de gebruiker data moet invoeren

om dan data terug te ontvangen. Als deze invoer niet gevalideerd wordt, dan is de kans reëel dat wanneer bijvoorbeeld het commando

```
SELECT * FROM USERS; DROP TABLE USERS;
```

wordt ingegeven, dit ook effectief wordt uitgevoerd met alle gevolgen nadien. (Acunetix, 2014)

Volgens Acunetix (2014) is een SQL-injectie één van de meest voorkomende aanvallen op de applicatielaag die vandaag voorkomen. Hierdoor is de kans dus vrij groot dat een webserver met een achterliggende webapplicatie hiermee te maken krijgt. Dus de factor *kans op een aanval* krijgt hier ook een 10 mee. De schade die deze aanval kan veroorzaken is natuurlijk ook zeer groot. Een goed gecoördineerde SQL-injectie kan de inloggegevens van alle gebruikers stelen en kan zelfs velden van de database verwijderen. Hierdoor krijgt de factor *schade van de aanval* een 9 mee. Dit brengt de totale waarde van de aanval op **90**, hetgeen zeer hoog is.

### **Metasploit telnet + putty**

In deze aanval wordt er gekeken via een port scan of poort 23 (telnet) open is bij een specifieke machine. Indien deze poort open is dat kan er via metasploit een exploit gezocht worden om via poort 23 binnen te breken in een machine. Dit kan gedaan worden door via een *dictionary attack* het wachtwoord en inlogaccount probeert te achterhalen van telnet op die specifieke machine. Als dit gelukt is kan er via *Putty* een verbinding worden gemaakt met de doelmachine. Metasploit is de grootste database van gekende exploits en het kan gebruikt worden door administrators om een server goed te beveiligen, maar helaas wordt het ook gebruikt door hackers die een server willen binnenbreken. (Majestro, 2014)

Dit is een aanval die moeilijk aan te leren is en die vele tijd en oefening vergt en hierdoor neemt de kans op een aanval een beetje af. Toch krijgt deze aanval nog bij de factor *kans op aanval* een 7 mee. De schade die deze aanval kan aanrichten is immens. Bij een succesvolle aanval zal de hacker volledige controle krijgen over het doelwit, in dit geval een webserver. Hij kon zo alle gegevens inkijken, kopiëren en verwijderen. Zo kan er gevoelige en geheime informatie doorgespeeld worden en kunnen er allerlei soorten chantage en spionage plaatsvinden. Bij de volledige controle over een machine zijn er veel zaken die een hacker kan doen dus hierdoor krijgt de factor *schade van de aanval* een 10 mee. Hierdoor komt de totale waarde van deze aanval op een **70** te staan.

### 4.2.2 Transportlaag

Dit is de derde laag van het TCP/IP-model en is hetzelfde als de 4de laag van het OSI-model. Deze laag is vooral gekenmerkt door de twee transportprotocollen TCP en UDP die hier op werken. De bedoeling van deze laag is om foutvrije berichten te verzenden tussen hosts. (Thomas, 2013)

#### Port scanning

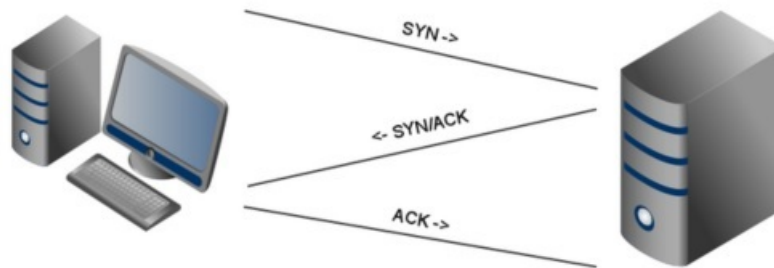
Een port scan kan gebruikt worden als een aanval, maar kan ook gebruikt worden voor de administrator te helpen. Bij een port scan wordt er gekeken bij een computer of een netwerk welke TCP -en/of UDP-poorten er allemaal open zijn en luisteren. Als aanvaller kan er zo gekeken worden waardat er mogelijkheden zijn om in te breken en als administrator kan er gekeken worden naar de zwakke plekken in het netwerk of op een computer/server. Via een port scan kan een administrator ook zien of er *bad ports* open zijn. Dit zijn poorten die open staan omdat er een trojan horse, DDoS-tool of een andere soort van kwaadaardige software op het systeem staat. Zo kan er ook tijdig ingegrepen worden. (Kessler, 2001)

Aangezien een webserver vanaf het openbare web bereikbaar is, is er een groot risico op port scans. Er bestaan zelfs bots die automatisch port scans uitvoeren bij willekeurige websites en alle zwaktes doorgeven aan de eigenaar. Hierdoor is de factor *kans op aanval* een 9. De schade daarentegen is zeer laag want een port scan zelf brengt geen schade toe tot een netwerk en is zelfs niet illegaal. Het uitbuiten van de exploits die deze port scan blootlegt, dat is wel illegaal. Het enigste wat een port scan doet is kijken door het raam van het huis, hetgeen niet strafbaar is. Pas wanneer er wordt ingebroken dan pas is het strafbaar en kan er schade zijn. Hierdoor is de factor *schade van de aanval* toch een 2 aangezien het potentiële zwaktes tentoonstelt. Dit brengt de totale waarde van deze aanval op **18**.

#### TCP SYN flood

Deze aanval is een soort van DOS-aanval waar de aanvaller de bekende *three-way handshake* misbruikt. Bij een normale three-way handshake wordt er een SYN-bericht gestuurd naar de server met de vraag om een connectie te verkrijgen. Daarna krijgt de gebruiker een SYN-ACK terug waarmee zijn request wordt geaccepteerd. Tot slot antwoordt de gebruiker met een ACK waarmee de verbinding tot stand wordt gebracht (zoals te zien is in figuur 4.2.2). Bij een TCP SYN flood-aanval worden er meerdere

SYN-berichten verzonden en worden er meerdere SYN-ACK berichten terug gestuurd naar de gebruiker maar deze stuurt geen enkele keer een ACK-bericht terug. Hierdoor blijven er half open verbindingen openstaan op een server en wordt er geheugen gebruikt op de server. Een voorbeeld van deze aanval is *Sockstress*. (Rouse, 2014)



Figuur 4.1: ThreeWayHandshake

Bron: <http://blogs.ixiacom.com/ixia-blog/tcp-portals-the-handshakes-a-lie/>

Dit is een aanval die veel kan voorkomen en die ook door gerespecteerd lid van de security community ? als zeer gevaarlijk wordt beschouwd. Het feit dat de webserver rechtstreeks in verbinding staat met het internet, wilt zeggen dat de kans zeer groot is dat deze aanval zal plaatsvinden dus daarom is de factor *kans op aanval* een 9. Een succesvolle aanval kan een server doen vastlopen en ook al wordt de aanval gestopt, de server kan alleen maar terug werken nadat deze handmatig opnieuw is opgestart. Dit zorgt ervoor dat de webserver onbereikbaar is tot dat er iemand naar de locatie gaat en op de shutdown-knop drukt en de server weer laat rebooten. Deze aanval kan geen gevoelige gegevens wissen of stelen, maar kan wel voor een lange downtime zorgen van een website/server. Daarom krijgt deze aanval een 7 mee bij de factor *schade van de aanval*. Hierdoor komt de waarde van deze aanval op **63** te staan.

### 4.2.3 Internetlaag

De internetlaag is de tweede laag van het TCP/IP-model en staat gelijk aan de 3de laag, de netwerklaag, in het OSI-model. Deze laag steekt de data in pakketten genaamd IP-datagrammen waar de bron -en eindbestemming van het pakket in verwerkt zitten. Deze laag is ook verantwoordelijk voor het routeren van deze pakketten. De protocollen die vooral worden gebruikt op deze laag zijn IP, ICMP en ARP. (Thomas, 2013)

### **Ping flood**

Een Ping flood is eigenlijk de oudste en meest primitieve vorm van een DOS-aanval want iedereen kan het doen en het is extreem gemakkelijk. Als een server een Ping flood-aanval te verduren krijgt, dan krijgt deze server zoveel ping requests dat deze het niet meer aankan omdat er teveel CPU-resources gebruikt worden. De aanvaller stuurt dan pings, via ICMP-pakketten, zonder te wachten op een antwoord. Hierdoor kan de server niet tijdig antwoorden en worden echte requests ook geblokkeerd. Dit kan leiden tot een immens vertraagde server en/of website. (Grid, 2010)

Bij een webserver hebben deze soort aanvallen een grote kans om uitgevoerd te worden door de verbinding die deze server heeft met het internet en omdat het zo gemakkelijk is om uit te voeren. Om een soortgelijke aanval te doen heeft een persoon weinig kennis nodig, dit maakt deze aanval zo angstaanjagend omdat iedereen het zou kunnen na een tutorial van 5 minuten. Hierdoor krijgt de factor *kans op aanval* een 10. De schade die deze aanval kan veroorzaken is echter vrij bescheiden. Het is niet dat een soortgelijke aanval een server kan plat gooien, maar het kan wel voor de nodige vertraging zorgen. Dit kan ervoor zorgen dat de website of server veel trager zal reageren op requests en dat de netwerkverbinding veel trager zal gaan. Aangezien deze aanval geen permanente schade kan veroorzaken maar enkel overlast, krijgt deze bij de factor *schade van de aanval* een 3 mee. Hiermee komt de totale waarde van de aanval op **30**.

### **ARP spoofing - Man in the middle**

Deze aanval wordt ook wel eens *ARP cache poisoning* of *ARP poison routing* genoemd. Dit is een aanval waar een aanval valse Address Resolution Protocol-berichten (ARP) over een LAN verzendt. Dit heeft als resultaat dat het MAC-adres van de aanvaller wordt gelinkt met een IP-adres van een echte computer in het netwerk. Vanaf deze link is geslaagd, zal de aanvaller alle data ontvangen die is bedoeld voor de computer waarvan de aanvaller het IP-adres gebruikt. De Man in the middle-aanval is de variant van ARP spoofing waar het verkeer tussen twee hosts eerst naar de hacker zijn machine wordt verzonden en nadat deze persoon de pakketten heeft kunnen bekijken (sniffen), dan wordt het verkeer naar de normale bestemming verzonden. Dit gebeurt zonder dat iemand er weet van heeft. Deze aanval kan alleen gebruikt worden, maar wordt in vele gevallen ook gebruikt in combinatie met een andere aanval. Bij een DoS-aanval kan ARP spoofing worden gebruikt om meerdere IP-adressen te linken aan één MAC-adres en zo het verkeer van al deze IP-adressen naar het doelsysteem waar het MAC-adres van is gebruikt. Zo wordt het doel overspoeld met verkeer. (Glynn, 2014)



Een soortgelijke aanval kan voorkomen op een webserver omdat deze rechtstreeks in verbinding staat met de router, maar deze is echter niet zo makkelijk uit te voeren als een ping flood. Hierdoor krijgt deze aanval bij de factor *kans op aanval* een 8. De schade die een hacker kan toebrengen aan een server of netwerk is dan weer vrij groot. Zo kan deze alle pakketten die worden verstuurd naar een "vergiftigde" host om zo gevoelige informatie te verkrijgen. Als een hacker de verbinding tussen bijvoorbeeld de baas en onderbaas van bedrijf A aanvalt, dan kan deze al het verkeer dat deze twee tussen elkaar uitwisselen inkijken zonder dat er iemand weet van heeft. Als deze personen dan gevoelige informatie uitwisselen met elkaar kan dit grote gevolgen hebben. Dit is dus een vrij gevaarlijke aanval die niet direct kan worden opgemerkt dus deze krijgt als factor *schade van de aanval* een 9. Dit brengt de totale waarde van deze aanval op **72**.

#### 4.2.4 Netwerктоegangslaag

Dit is laag 1 van het TCP/IP-model en is een samenvoeging van de fysieke -en datalinklaag bij het OSI-model, die daar laag 1 en 2 zijn. Hier worden de details meegegeven over hoe data precies over een netwerk moet verzonden worden. De protocollen die hier het meeste voorkomen zijn Ethernet, Token Ring en Frame Relay.

##### Keylogging

Bij dit soort aanvallen wordt input van het toetsenbord opgeslagen zonder dat de gebruiker dit doorheeft. Deze aanval wordt vooral gebruikt om zo aan wachtwoorden en gevoelige informatie te komen. Keylogging hoeft ook niet direct illegaal te zijn, er zijn veel varianten van keylogging die in softwareprogramma's worden gebruikt om zo een beter gebruikerservaring aan te bieden. Ook is er legale software waarmee administrators kunnen meekijken met wat de gebruikers op een netwerk allemaal doen. Natuurlijk is de lijn tussen het controleren van de werknemers en spionage een dunne lijn. Legale software kan zo ook gebruikt worden om illegale zaken uit te voeren. In tegenstelling tot de meeste aanvallen die eerder al besproken zijn, kan software voor deze aanval op de vrije markt gekocht worden en dat maakt het ook gevaarlijker. Bij een soortgelijke aanval krijgt een hacker de keylogger-software op de doelmachine en kan zo wachtwoorden of bankinformatie te weten komen. Een bekend voorbeeld van deze aanval is het keylogger-incident bij een grote Scandinavische bank waar 1 miljoen dollar is gestolen van bepaalde accounts. De aanvaller stuurde mails in de naam van de bank naar bepaalde klanten met de melding dat deze nieuwe anti-spamsoftware moesten installeren. Bij het downloaden van de bijlage werd er een keylogger geïnstalleerd en zo kreeg de aanvaller de bankinformatie van al deze

klanten. (Grebennikov, 2007)

Deze soort aanval is niet moeilijk om uit te voeren en komt vrij veel voor. Op een server zal deze echter veel minder voorkomen aangezien er op een server zo goed als nooit bestanden zullen gedownload worden van het internet of e-mails en al zeker niet van niet-vertrouwde bronnen. Een keylogging-aanval zal vooral plaatsvinden op een client. Hierdoor krijgt de factor *kans op aanval* een 2 mee. De schade die deze aanval kan aanrichten is dan weer vrij groot. Als een server/computer slachtoffer wordt van een keylogging aanval, kunnen wachtwoorden en gebruikersnamen gestolen worden om zo veel schade aan te richten of gevoelige informatie te stelen. Hierdoor krijgt de factor *schade van de aanval* een 9 mee. De totale waarde van deze aanval komt dan op **18** te staan.

## 4.3 Prioriteiten

Nu er een opsomming is gemaakt van de verschillende bedreigingen kunnen er prioriteiten gesteld worden bij het onderzoeken van al deze bedreigingen. Er kan nu een tabel gemaakt worden met de naam van de bedreiging en de bijhorende waarde die deze heeft megekregen. Hoe groter de waarde, hoe hoger de aanval in de tabel zal geplaatst worden. Zo kunnen de aanvallen met het grootste risicogehalte eerst onderzocht worden.

Bedreiging	Risicowaarde
SQL-injectie	90
ARP spoofing - Man in the middle	72
Metasploit telnet + putty	70
TCP SYN flood	63
Laag 7 DoS-aanvallen	54
Ping flood	30
Port Scanning	18
Keylogging	18
DNS Poisoning	9

Tabel 4.1: Ordening bedreiging op risicogehalte

# Hoofdstuk 5

## Penetration Testing

### 5.1 Applicatie laag

#### 5.1.1 Brute force Hydra-aanval

##### **Uitvoering en schade**

Hydra is één van de bekendste en meest gebruikte tools die Kali Linux te bieden heeft en deze is makkelijk terug te vinden op de aanvallersmachine aangezien deze tool bij de top 10 van meest gebruikte tools staat. Met Hydra kan een persoon wachtwoorden kraken van desktops of servers. Het principe is vrij simpel, de enige benodigheden zijn een Kali-machine, het ip-adres van het slachtoffer en een woordlijst die zelf kan gemaakt worden of die van het internet kan gehaald worden. In deze aanval wordt de naam van een administrator-account meegegeven en een lijst van verschillende woorden of wachtwoorden die één voor één worden uitgetest. Om deze lijst nog efficiënter te maken, kan een hacker gebruik maken van social engineering waar hij persoonlijk informatie over een gebruiker opzoekt, hetgeen zeer makkelijk is via facebook, en deze informatie dan gebruikt om wachtwoorden te vormen. Dit kan variëren van geboorteplaats tot de namen van kinderen of ouders. Al deze informatie wordt in lijsten gestoken met verschillende soorten combinaties om een groter succesratio te kennen. (Wilde, 2013)

Voordat deze aanval kan uitgevoerd worden moet de aanvaller eerst de naam van het administrator-account weten. Standaard is dit „Administrator” en als netwerk-beheerders dit niet aangepast hebben dan is het zeer makkelijk om met deze aanval binnen te dringen. In dit geval beschikt de aanvaller over het eigen gemaakte account

met de naam „BaeleAdministrator”. In de aanvallersmachine wordt er allereerst een woordenlijst gedownload of aangemaakt. In dit geval wordt er een zelfgemaakte woordenlijst gebruikt aangezien zo een internetlijst 100 000’en verschillende combinaties hebben die zeer lang duren om helemaal door te lopen. In dit geval bevat de zelfgemaakte woordenlijst 5 woorden: „test, test123, Baele123, groen, bos”. In dit geval is Baele123 het echte wachtwoord. Daarna wordt er in het terminalvenster dit lijntje ingetypt: „*hydra -t 1 -l BaeleAdministrator -P /root/woordenlijst.txt. -vV <IP-ADRES slachtoffer> ftp*”. Daarna wordt elk woord in de lijst apart uitgetest totdat er een juiste combinatie is of tot de lijst doorlopen is. (Moon, 2013)

De schade die deze aanval aan kan richten is immens. Bij een succesvolle aanval weet de aanvaller het wachtwoord van een account met administrator rechten. Hiermee kan hij zich aanmelden via o.a. verbinding met extern bureaublad en kan de aanvaller aan alles wat zich op een server bevindt. Het spreekt voor zich dat dit niet goed is en dat dit ervoor kan zorgen dat er geheime bestanden worden gestolen of dat het netwerk wordt platgelegd en noem maar op.

### **Bescherming en preventie**

De best practices die eerder besproken zijn, zijn voldoende om deze aanval af te weren. Hoe complexer een wachtwoord is, hoe kleiner de kans is dat het wachtwoord zich in de woordenlijst zal bevinden. Er bestaan natuurlijk gigantisch grote woordenlijsten waar bijna alle mogelijke combinaties in gebruikt worden, maar deze duren veel langer om uit te voeren. Hoe complexer het wachtwoord, hoe langer de aanval ook moet duren dus hoe meer kans er is dat de aanval wordt opgemerkt of wordt onderbroken.

Ook een best practice is om het default account „Administrator” uit te schakelen en een zelfgemaakt account te maken. Als dit wordt gedaan dan moet een aanvaller al kennis hebben over het netwerk en de server om te weten welk account er kan gekraakt worden. Als het default account wordt gebruikt dan kan iedereen op elke plaats in de wereld binnen breken zonder dat de persoon iets weet van een server. Dit in combinatie met een groepsbeleidobject die het account blokkeert na 3 foutieve pogingen zorgt ervoor dat deze aanval geen schijn van kans heeft.

### **5.1.2 SQL injection**

#### **Uitvoering en schade**

Bij een SQL-injectie worden er SQL-statements die een slechte validatie hebben gebruikt om een website binnen te dringen. Deze aanval is zo gevaarlijke en destructief dat deze in 2013 volgens Cisco (2013) zelfs op de eerste plaats stond van meest gevaarlijke bedreigingen voor web applicaties. Via een SQL-injectie kan een aanval o.a. de volgende zaken doen:

- Authenticatie omzeilen om zo in te loggen op de applicatie met administrator bevoegdheden.
- Gevoelige/geheime informatie in een database bekijken en gebruiken.
- Malware plaatsen in de database of op de website.
- Cruciale gegevens verwijderen.

Op de Kali-aanvallersmachine wordt er voor deze aanval gebruik gemaakt van sqlmap. Er zijn meerdere tools om een SQL-injectie uit te voeren, maar in dit voorbeeld wordt deze tool gebruikt. Allereerst moet de naam van de database gekend zijn en dit kan makkelijk gevonden worden door „sqlmap -u www.baele.be -dbs” in te typen. Nu dat de naam van de database bekend is, moeten de tabellen gekend zijn en dit gebeurt via „sqlmap -u www.baele.be -D TestDatabase -tables” waar „TestDatabase” de naam van de database voorstelt. Nu is er een hele lijst aan tabellen zichtbaar en kan er een willekeurige tabel geselecteerd worden. In dit geval wordt de tabel „Gebruikers” genomen. Hierna wordt er een willekeurige kolom genomen uit deze tabel via „sqlmap -u www.baele.be -D TestDatabase -T Gebruikers -columns”. Nu is er de mogelijkheid om de hele tabel te „dumpen” of enkele velden in een lokale map. Dit wordt gedaan via „sqlmap -u www.baele.be -D TestDatabase -T Gebruikers -dump”. Nu kan er gebrowsed worden naar de locatie die staat beschreven in het terminalvenster om te kijken wat er allemaal opgeslaan is en daar is te zien dat de hele tabel aanwezig is.

#### **Bescherming en preventie**

Het spreekt voor zich dat deze soort aanval veel schade kan toebrengen. Gelukkig is het ook mogelijk om een webapplicatie te beschermen tegen mysql-injecties. Deze bescherming is codegericht en is dus belangrijk voor de persoon die de webapplicatie en database heeft aangemaakt. Deze persoon moet ervoor zorgen dat de code voldoende getest is en foutvrij is. Volgens Angus (2005) zijn er verschillende manieren om de SQL-code foutvrij te maken. Dit kan gedaan worden door het crypteren van

gevoelige data, de database installeren en gebruiken met een account die zo weinig mogelijk bevoegdheden heeft. Enkel de bevoegdheden die nodig zijn zouden op dat account moeten zitten. Het administrator-account gebruiken wordt dan ook afgeraden.

Wat ook belangrijk is, is dat de data gevalideerd wordt, dat er geparameteriseerde queries en „stored procedures” worden gebruikt, dat de data opnieuw wordt gevalideerd in de stored procedure en dat de error boodschappen niets weggeven over de interne architectuur van de applicatie of de database. Hier wordt er niet te diep op ingegaan omdat dit niet echt een taak is voor de netwerkbeheerder maar eerder voor de programmeur of applicatiebeheerder.

## 5.2 Transportlaag

### 5.2.1 Sockstress DDOS-aanval

#### **Uitvoering en schade**

Een fysieke machine kan onbruikbaar gemaakt worden door een simpele aanval genaamd „sockstress”. Deze aanval heeft de laatste tijd enorm gewonnen aan populariteit in het hackersmilieu en dus ook in de kringen van netwerkbeveiligers. Deze methode wordt gebruikt om servers aan te vallen over het internet door middel van TCP. Deze methode zorgt ervoor dat het lokale geheugen zoveel aanvragen moet behandelen dat deze langzaam maar zeker volloopt zodat de server vastloopt en onbruikbaar wordt. Dit wordt ook wel een DOS (Denial Of Service)-aanval genoemd.

Op de aanvallersmachine, in dit geval de eerder geconfigureerde Kali Linux-machine, worden er twee verschillende „command lines (cmd)” geopend. In de eerste cmd wordt er „*nmap <ipadres slachtoffer>*” getyped om te kijken welke poorten van het slachtoffer die open zijn. De open poorten worden dan ergens genoteerd want deze zijn later nog nodig. Nadat deze zijn genoteerd, wordt er een script genaamd „*./arppoi*” geopend in dit terminalvenster. Dit scriptje is te vinden op het internet en de code is te zien in de appendix. De bedoeling van dit script is ARP spoofing. ARP spoofing is een techniek die door veel hackers wordt gebruikt en waar er vermomde ARP-berichten in een lokaal netwerk worden verzonden. De bedoeling is om het MAC-adres van de aanvaller te associëren met het IP-adres van een host, bijvoorbeeld een default gateway of server, zodat al het verkeer dat bedoeld is voor dat specifieke adres naar de aanvaller wordt verzonden.

Nu dat scriptje draait in het een terminalvenster, hoeft er in het andere venster maar één lijntje ingevuld worden. „./sockstress -A -C -1 -d <IP van target> -m -1 -Ms -p <alle opgeschreven poorten> -r 100000 -s 172.16.246.0/25 -vv”. Dit werkt ook alleen maar als sockstress is gedownload en als je navigeert naar de sockstress-map. Nu kan er gekeken worden naar de server en is er te zien dat het RAM-geheugen dat in gebruik is op de server exponentieel aan het stijgen is. Als dit de maximume waarde bereikt dan zal de server vastlopen en kan er niets meer op gedaan worden. De engiste manier om de server terug aan de praat te krijgen is door manueel de uit-knop in te drukken en hem dan weer op te starten.

### **Bescherming en preventie**

De best practices die op de server zijn geïmplementeerd zijn in dit geval niet voldoende en dus moet er een oplossing gevonden worden. De oplossing in dit geval is vrij simpel. Dit kan gedaan worden door het blokkeren van een IP-adres als het meer dan 10 connecties met een poort maakt in minder dan 30 seconden. Dit wordt gedaan door een simpel lijntje in te typen in de router command line „iptables -I INPUT -p tcp -dport 80 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j DROP”. Aangezien de server enkel handmatig kan worden afgesloten, is de kans reeël dat er gegevensverlies is. Daarvoor is het belangrijk dat dit direct wordt bekeken nadat de server opnieuw is opgestart zodat er direct een restore kan plaatsvinden als dit nodig is. Hiervoor zijn de best practices wat betreft back-ups wel voldoende.

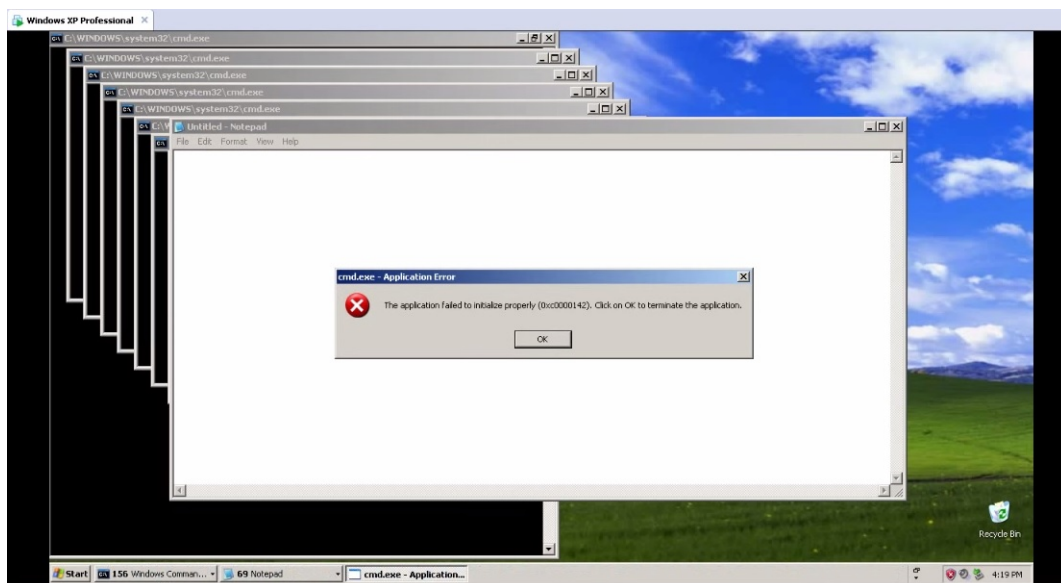
## **5.3 Netwerklaag**

### **5.3.1 Malware applicaties**

#### **Uitvoering en schade**

Malware is een afkorting van „malicious software” en betreft alle software die als bedoeling heeft om een netwerk of computere schade toe te brengen. Er zijn verschillende soorten malware waaronder virussen en spyware behoren tot de bekendste. (Moir, 2003). In dit geval wordt er een simpel malware-bestand aangemaakt en op de server geplaatst. Hier wordt er gesimuleerd dat de administrator een schadelijk stukje software download op het internet en deze dan laat uitvoeren.

Door het typen van de volgende tekst in een kladblokbestand kan er een virus aangemaakt worden: „@echo off :A start virus.bat start notepad.ext goto A” en sla dit bestand op als „virus.bat”. Dit simpel virus zorgt ervoor dat het RAM-geheugen van een computer of server binnen de minuut helemaal volloopt. Het programma start elke keer een commandprompt op en elke keer als dit gebeurt wordt er ook een nieuwe kladblokapplicatie geopend. Dit gebeurt oneindig veel keer tot het RAM-geheugen vol zit en de server of computer vastloopt. Hierna kan een apparaat enkel manueel worden afgesloten om het weer aan de praat te krijgen.



Figuur 5.1: Voorbeeld Malware-aanval

### Bescherming en preventie

Het spreekt voor zich dat de best practice voor een anti-virus die eerder al besproken is in 99% genoeg. Als de anti-virus software up-to-date is en dagelijks wordt geupdate, dan is er zo goed als geen risico dat er bedreigingen op de computer komen. Indien er toch een bedreiging door de anti-virus geraakt, is het aan de persoon in kwestie om verstandig te zijn in wat deze precies open doet en downloadt van het internet. Een veilige extra best practice kan zijn om gebruikers niet de permissie geven om programma's te installeren op de computer. Zo zal er altijd een administrator nodig zijn die zijn toestemming moet geven of een specifiek stukje software mag geïnstalleerd worden.

### LOGS



# Hoofdstuk 6

## Post mortem

### 6.1 Manueel

#### 6.1.1 RAM-geheugen

Manueel kan er makkelijk gekeken worden naar het RAM-geheugen dat wordt gebruikt door „ctrl+alt+del” in te drukken of door met de rechtermuisknop te drukken op het Windows-logo linksonder op het scherm en „Taakbeheer” te selecteren. Hierin zijn er verschillende tabbladen en het RAM-geheugen kan gevonden worden in het tabblad „Prestaties” waarna er kan geklikt worden op „Geheugen” in de linkerkolom. In dit venster is het geheugengebruik voor de laatste 60 seconden zichtbaar en wordt deze elke seconden ververs. Als de curve per seconde omhoog gaat dan kan er sprake zijn van een Sockstress DDOS-aanval en kan er tijdig gehandeld worden. Het manueel bekijken van het RAM-geheugen kan handig zijn als de server opeens trager begint te werken om te kijken of het probleem niet hier ligt.

#### 6.1.2 Geblokkeerde accounts

Na 3 foutieve inlogpogingen wordt een gebruikersaccount direct in een „lock” gestoken en moet deze door de administrator, of iemand met de benodigde rechten, weer uit deze lock gehaald worden. Om te kijken hoeveel en welke accounts er precies in een lock zitten, kan een zeer simpel powershell-commando uitgevoerd worden. Bij het openen van Powershell en met het volgende lijntje code worden alle geblokkeerde accounts weergegeven: „Search-ADAccount -LockedOut”.

Als alle accounts die in een lock zitten we op actief mogen staan, kan dit ook gedaan worden met een simpel lijntje code: „Search-ADAccount -LockedOut | Unlock-ADAccount”. Indien niet alle accounts terug actief mogen worden, kan er nog een stukje toegevoegd worden aan de code zodat er voor elk gelocked account een bevestiging moet gegeven worden: „Search-ADAccount -LockedOut | Unlock-ADAccount -Confirm”. Voor de accounts die weer op actief mogen staan moet er een „y” ingetyped worden en voor de accounts die in een lock moeten blijven wordt er een „n” getyped.

### **6.1.3 Malware**

Om manueel te kijken of er malware aanwezig is op de server is er anti-virus-software nodig. Er zijn honderden verschillende keuzes en bij elke keuze kan er manueel een scan gestart worden en kan er manueel gekeken worden welke bedreigingen er gevonden zijn en welke risico's er aanwezig zijn. Deze kunnen dan manueel verwijderd of in quarantaine geplaatst worden.

## **6.2 Automatisch**

### **6.2.1 Prestatiemeter**

Met behulp van de prestatimeter-tool kunnen bepaalde zaken makkelijk in de gaten gehouden worden. In de prestatimeter kunnen er gegevensverzamelaarset aangemaakt worden naar persoonlijke voorkeur die het mogelijk maken om elk aspect apart onder de loep te nemen en deze in log files op de slaan.

#### **RAM-geheugen**

De eerste gegevensverzamelaarset die zeer handig is om te maken is één die het gebruik van het RAM-geheugen in de gaten houdt. Deze kan worden ingesteld door allereerst naar de tool „prestatimeter” te gaan en te rechterklikken op „Prestatiemeter” onder het tabblad „controlehulpprogramma's”. Daarna moet er onder de keuze „Nieuw” gekozen worden voor „gegevensverzamelaarset”. Nu kan er een gepaste naam gekozen worden voor deze set, in dit geval is „RAMGeheugen” een goede naam aangezien we hier het RAM-geheugen gaan bekijken. Bij de volgende keuzes mag er 2x op „volgende” gedrukt worden.

Nu is de set aangemaakt en is deze terug te vinden onder het tabblad „Gedefinieerd door de gebruiker” en moet er hier op gedubbelklikt worden tot „Logboek voor Systeemmonitor” zichtbaar is en dan moet er hier op gedubbelklikt worden. Nu zijn de eigenschappen van de set zichtbaar en kunnen er via „Toevoegen” specifieke parameters toegevoegd worden. In dit geval is het handig om naar „Geheugen” te gaan en daar te kiezen voor „Beschikbare megabytes” en „Percentage toegewezen bytes in gebruik”. Nadat deze zaken zijn toegevoegd kan er 2x geklikt worden op de OK-knop. Nu moet er met de rechtermuisknop op de juist aangemaakte set geklikt worden om dan op „starten” te klikken, dit een 10-tal minuten te laten lopen en daarna op „stoppen” te drukken. Nu kan er gekeken worden naar het tabblad „rapporten” en „gedefinieerd door de gebruiker” naar wat deze actie juist heeft opgebracht. In dit scherm is er een bestand zichtbaar (met de bijhorende datum) die bij het dubbelklikken alle parameters laat zien met de bijhorende tijd in een mooie grafiek. Hier is duidelijk wanneer precies er pieken zijn in het gebruik van het RAM-geheugen en wanneer deze precies een bepaalde grens overschrijdt.

### **foutieve inlogpogingen**

Het is mogelijk om foutieve aanmeldpogingen op de server te registreren in logbestanden. Dit kan gedaan worden door naar het „lokaal beveiligingsbeleid” te gaan en daar in de beveiligingsinstellingen bij „lokaal beleid” en „controlebeleid” kan er gekozen worden voor „aanmeldingsgebeurtenissen controleren”. Hierin kan er gekozen worden om mislukte pogingen te registreren. Hetzelfde wordt gedaan voor „accountbeheer controleren”. Elke keer dat er nu iemand wilt inloggen en deze geeft een foutief antwoord, dan wordt er een logbestand aangemaakt.

# Hoofdstuk 7

## Conclusie

De conclusie zal geschreven worden na de feedback, als de laatste wijzingen uitgevoerd zijn!

# Bibliografie

- Acunetix (2014). Sql injection: What is it? *Acunetix*.  
<https://www.acunetix.com/websitesecurity/sql-injection/>.
- Angus, C. (2005). *SQL Injection and some tips on how to prevent them*. <http://www.codeproject.com/Articles/9378/SQL-Injection-Attacks-and-Some-Tips-on-How-to-Prev>.
- Blagov, M. (2014). Denial of service. *Incapsula*.  
<https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html>.
- Cisco (2013). *SQL Injection*. [http://www.cisco.com/web/about/security/intelligence/sql\\_injection.html](http://www.cisco.com/web/about/security/intelligence/sql_injection.html).
- Cott, R. (2012). Best practices for securing your web server. *ServerBeach*. <http://www.serverbeach.com/resources/Best-Practices-For-Securing-Your-Web-Server>.
- Darmanin, G. (2014). 8 tips to secure your iis installation. *Acunetix*.  
<http://www.acunetix.com/blog/articles/8-tips-secure-iis-installation/>.
- Gibson, D. (2011). *Exploring common web server attacks*.  
<http://www.pearsonitcertification.com/articles/article.aspx?p=1713591>.
- Glynn, F. (2014). Arp spoofin. *Veracode*. <http://www.veracode.com/security/arp-spoofing>.
- Grebennikov, N. (2007). Keyloggers: How they work and how to detect them. *Securelist*. <https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/>.
- Grid, G. (2010). *Tutorial: How to DoS Attack (Ping Flooding)*.  
<http://ghostgrid.blog.com/2010/12/16/ping-flooding/>.

- Herring, D. (2014). *How to Install Microsoft Security Essentials on Windows Server 2012 and 2012 R2*. <http://www.puryear-it.com/blog/2014/06/16/install-microsoft-security-essentials-windows-server-2012-2012-r2/>.
- Hoffman, C. (2015). Htg explains what is dns cache poisoning. *HowToGeek*. <http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/>.
- Kessler, G. C. (2001). Port scanning: It's not just an offensive tool anymore. *Information Security Magazine*. [http://www.garykessler.net/library/is\\_tools\\_scan.html](http://www.garykessler.net/library/is_tools_scan.html).
- Majestro (2014). *Telnet Login BruteBrute (metasploit + putty)*. <https://www.youtube.com/watch?v=KUyUICumTRA>.
- Maman, D. (2013). Sql server security best practices. *GreenSQL*.
- Microsoft (2013). *Security Best Practices for IIS 8*. <https://technet.microsoft.com/en-us/library/jj635855.aspx>.
- Moir, R. (2003). Defining malware. *Microsoft technet*. <https://technet.microsoft.com/en-us/library/dd632948.aspx>.
- Moon, S. (2013). *Crack ftp passwords with Hydra*. <http://www.binarytides.com/crack-ftp-passwords-with-thc-hydra-tutorial/>.
- Nabors, E. (2013). *Managing the Windows Server 2012 Firewall*. [http://www.rackspace.com/knowledge\\_center/article/managing-the-windows-server-2012-firewall](http://www.rackspace.com/knowledge_center/article/managing-the-windows-server-2012-firewall).
- Nuckolls, J. (2011). *Create ASP.Net web app and SQL server database*. [https://www.youtube.com/watch?v=\\_gqpBLNo7wo](https://www.youtube.com/watch?v=_gqpBLNo7wo).
- Poley, J. (2013). Best practices for keeping the web server data protected. *Stackoverflow*. <http://stackoverflow.com/questions/18525927/best-practices-for-keeping-the-web-server-data-protected>.
- Posey, B. (2011). 10 best practices for windows security. *TechRepublic*. <http://www.techrepublic.com/blog/10-things/-10-best-practices-for-windows-security/>.
- Rouse, M. (2014). Syn flood (half open attack). *TechTarget*. <http://searchsecurity.techtarget.com/definition/SYN-flooding>.
- Siddharth, S. (2006). *Five common web application vulnerabilities*. <http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities>.

- Sima, C. (2005). Security risk assessment and management in web application security. *WebProNews*. <http://www.webpronews.com/security-risk-assessment-and-management-in-web-application-security-2005-11>.
- Stanek, W. R. (2009). *Windows Server 2008 Administrator's pocket cons*. Microsoft, 2de editie edition. <https://technet.microsoft.com/en-us/magazine/ff741764.aspx>.
- Thomas, J. (2013). Four layers of tcp/ip model, comparison and difference between tcp/ip and osi models. *Omnisecu*.
- Vialle, P. (2012). Security best practices to protect internet facing web servers. *Microsoft*. <http://social.technet.microsoft.com/wiki/contents/articles/13974.security-best-practices-to-protect-internet-facing-web-servers.aspx>.
- Wiener-Bronner, D. (2014). Report shows cyber crime is on the rise. *The Wire*. <http://www.thewire.com/technology/2014/04/report-shows-cyber-espionage-is-on-the-rise/361024/>.
- Wilde, B. (2013). *Hacking Tutorial: Brute Force Password Cracking*. <https://blog.udemy.com/hacking-tutorial/>.

## Lijst van figuren

2.1	Proefopstelling . . . . .	8
3.1	Alle toegestane uitgaande verbindingen . . . . .	15
3.2	Voorbeeld van succesvolle scan met volgende geplande scan . . . . .	16
3.3	Alle modules die geactiveerd blijven . . . . .	18
3.4	De term OPTIONS wordt niet toegestaan . . . . .	19
3.5	Instellingen voor dynamische IP-beperking . . . . .	20
4.1	ThreeWayHandshake . . . . .	27
5.1	Voorbeeld Malware-aanval . . . . .	36



# Lijst van tabellen

4.1	Ordering bedreiging op risicogehalte . . . . .	30
-----	--	----