



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

1	Inleiding	4
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
2	Methodologie	7
3	Opzetten servers met best practises beveiliging	9
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	Inloggen	13
3.4.3	Updates	13
3.4.4	Backup	13
3.4.5	Firewall	14
3.4.6	Anti-virus	14
3.5	IIS best practices WebServer	14
3.5.1	Dedicated server	14
3.5.2	Inetpub	15
3.5.3	Modules	15
3.5.4	Opties methode uitschakelen	15
3.5.5	Dynamische IP restricties	15
3.5.6	Request Filtering Rules	16
3.5.7	Inschakelen logs	16
3.6	SQL Server best practices WebServer	16

4	Risico-analyse	17
4.1	Assets	17
4.2	Mogelijke bedreigingen	17
4.2.1	Applicatielaag	18
4.2.2	Transportlaag	18
4.2.3	Internetlaag	18
4.2.4	Netwerklaag	18
4.2.5	Fysieke laag	18
4.3	Netwerkscanner	19
4.4	Kwestbaarheidsscanner	19
4.5	Packet capture tools	20
5	Penetration Testing	23
5.1	Applicatie laag	23
5.1.1	Brute force Hydra-aanval	23
5.1.2	SQL injection	25
5.2	Transportlaag	26
5.2.1	Sockstress DDOS-aanval	26
5.3	Netwerklaag	27
5.3.1	Malware applicaties	27
6	Post mortem	29
6.1	Manueel	29
6.1.1	RAM-geheugen	29
6.1.2	Geblokkeerde accounts	29
6.1.3	Malware	30
6.2	Automatisch	30
6.2.1	Prestatiemeter	30
7	Conclusie	32

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 beveliging 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

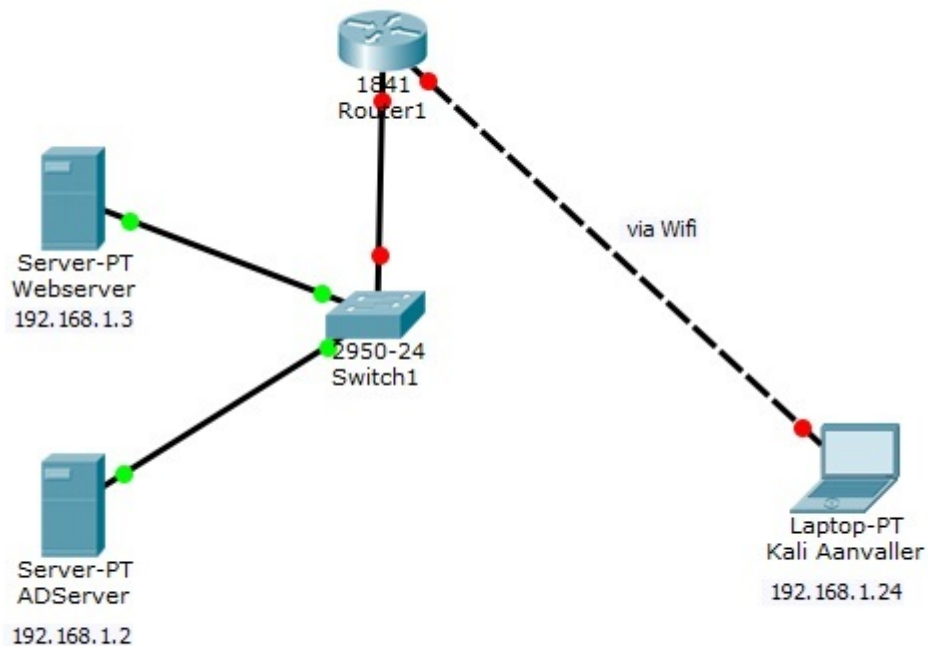
van de administrator om ervoor te zorgen dat aanvallen makkelijk terug te vinden zijn ofwel manueel ofwel automatisch zodat deze tijdig kunnen onderbroken worden of niet meer zullen voorvallen.

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 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 opgewaard 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).

3.4.2 Inloggen

Eén van de eerste zaken dat moet gebeuren is het uitschakelen van de inlognaam "Administrator" een eigen administrator login maken en deze dan toevoegen aan de groep „Administrators” zodat deze dezelfde rechten heeft als het net uitgeschakelde account. De reden voor deze maatregel is om brute force aanvallen tegen te gaan. Elke IT'er kent het „Administrator-account” en deze is dan kwetsbaar voor aanvallen die proberen om het wachtwoord te kraken. Als het account is uitgeschakeld dan moet er al een accountnaam geweten zijn voordat er brute force aanvallen kunnen plaatsvinden. In dit geval is er een account aangemaakt genaamd „BaeleAdministrator” en is deze lid geworden van de groepen *Administrators*, *Domeinadministrators* en *domeincontrollers*. Ook is het gebruikelijk dat er een complex wachtwoord wordt gebruikt voor dit account. Er wordt aangeraden om hoofdletters, kleine letters, cijfers en speciale tekens te gebruiken in het wachtwoord. Een andere best practice is om het wachtwoord regelmatig, maandelijks of half jaarlijks, eens te wijzigen. Ten slotte is het ook een best practice dat er bij de groepsbeleidsobjecten wordt ingesteld dat een account wordt geblokkeerd nadat er 3x verkeerd is ingelogged.

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.

3.4.6 Anti-virus

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. Het is ook belangrijk dat de software dagelijks wordt geupdate zodat er geen nieuwe bedreigingen ongezien binnen geraken. Best wordt er 's nachts, als niemand de server gebruikt, automatisch een anti-virus scan gedaan om te kijken of alles nog steeds veilig is.

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. (Microsoft, 2013)

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.

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.

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.

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.

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.

3.6 SQL Server best practices WebServer

Hoofdstuk 4

Risico-analyse

Het uitvoeren van een risico-analyse kan in verschillende stappen onderverdeeld worden. Allereerst moet er een opsomming zijn van alle *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 bijkomend:

- Internet Information Services 8
- Externe toegang, routing
- Microsoft SQL Server Express 2014

4.2 Mogelijke bedreigingen

De soorten bedreigingen kunnen ingedeeld worden per laag van het OSI-model. Hierdoor kan er structureel gekeken worden naar elke laag om zo te kijken welke bedrei-

gingen 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.

4.2.1 Applicatielaag

applicatie services enz

Applicatie laag DDOS-aanvallen [https : //conference.apnic.net/data/37/l7ddos_apricot₁393257782.pa](https://conference.apnic.net/data/37/l7ddos_apricot_1393257782.pdf)
[https : //www.youtube.com/watch?v = BYKnBki2WTc](https://www.youtube.com/watch?v=BYKnBki2WTc)

layer 4 ddos = 100 gebruikers leggen 1 site plat (veel gebruikers met 1 doelwit) al de bandbreedte wordt gebruikt. low orbit ion canon, layer 7 dos = 1 gebruiker legt site plat

vb. R-U-Dead-Yet, niet complete dingen sturen naar IIS, maakt de server unavailable
Keep-alive DoS, Keep-dead DoS, gebruikt CPU XerXes DOs, lokale host maakt aanvalt en is anoniem en geen firewall kan beveiligen link-local dos

4.2.2 Transportlaag

TCP en UDP werken hier

4.2.3 Internetlaag

IP protocol werkt hier, zorgt voor netwerkadressen en routing

4.2.4 Netwerklaag

Ethernet, token-ring, individuele netwerk protocollen

4.2.5 Fysieke laag

hardware

4.3 Netwerkscanner

Jackson (2010) schreef dat nmap de netwerk -en scanningtool is die de meeste beveiligingsexperts gebruiken. Deze is gratis, open source applicatie is beschikbaar op alle Windows besturingssystemen. In deze situatie wordt er ook gebruik gemaakt van deze bekende tool. Nmap kan gebruikt worden om een netwerk van alle groten te scannen. Deze tool werkt vrij simpel, als je nmap voorziet van een IP-adres dan kan je alle „open deuren” of poorten te zien krijgen van een specifiek IP-apparaat of een range van IP-apparaten. Dit gebeurt door een ping sweep die de hosts zal identificeren die actief zijn op een netwerk en voor deze actieve hosts zal er gekeken worden welke services er antwoorden. (Messer, 2007).

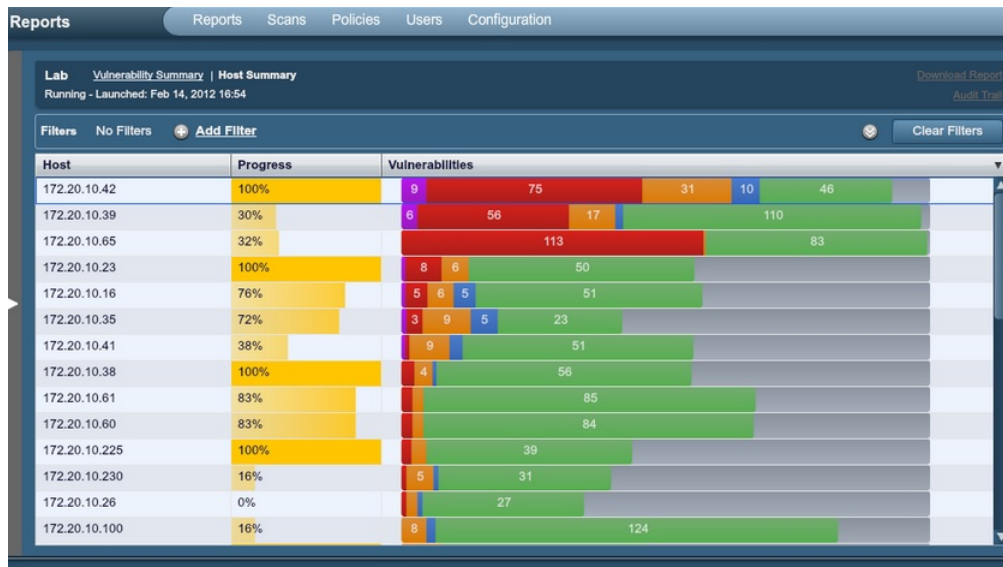
Met behulp van een netwerkscanner, in dit geval nmap, kan er gekeken worden welke poorten kunnen geëxploit worden. Hackers gebruiken dit om te zoeken naar open poorten waardoor ze binnen een computer of netwerk kunnen breken m.b.v. een exploit. Op de webserver zullen er meer poorten open zijn dan op de ADServer die ook domeincontroller is. Bijvoorbeeld poorten 80 en 443 zijn specifiek voor een webserver. In het geval dat er poorten open zijn die niet open moeten staan, dan kunnen deze worden gesloten door naar het takenbeheer te gaan en te kijken welke service er bij deze poort hoort. Hoort deze service niet thuis op het netwerk of op de computer, dan kan deze verwijderd worden. Dankzij het uitvoeren van een port scan kan er gekeken worden of er op een server poorten open staan die vatbaar zijn voor een aanval. Indien deze tijdig worden gevonden kan een potentiële aanval afgewend zijn.

4.4 Kwestbaarheidsscanner

Nessus is volgens Jackson (2010) een populaire kwetsbaarheidsscanner die zoekt naar zwakke plekken in besturingssystemen, netwerkkapparaten en applicaties. Deze scans gebeuren via een database zodat alle nieuwste bedreigingen direct kunnen gevonden worden. Daarom is het ook belangrijk dat Nessus wekelijks of dagelijks wordt geupdate zodat elke scan zo efficiënt mogelijk kan gebeuren. Deze soort scan is een uitgebreidere versie van de nmap-scan.

Allereerst moeten er policies ingesteld worden die zullen gebruikt worden om het netwerk in te schatten. In deze sectie worden ook plugins ingesteld die het hart van Nessus voorstellen. Er kunnen duizenden plugins worden ingesteld, maar om de snelheid van de scan te verbeteren is het gebruikelijk om enkel de plugins te pakken die van toepas-

sing zijn om het te onderzoeken netwerk.



Figuur 4.1: Voorbeeld Nessus-scan (Bron: <http://soft365.vn>)

Nadat deze zijn ingesteld kan er één of meerdere IP-adressen ingegeven worden om de bijhorende apparaten te scannen. Voor elke host die is gescannend komt er een lijst met alle zwaktes op een overzichtsscherm. Deze zwaktes worden gecatalogiseerd naargelang de grootte. (Afbeelding 4-1)

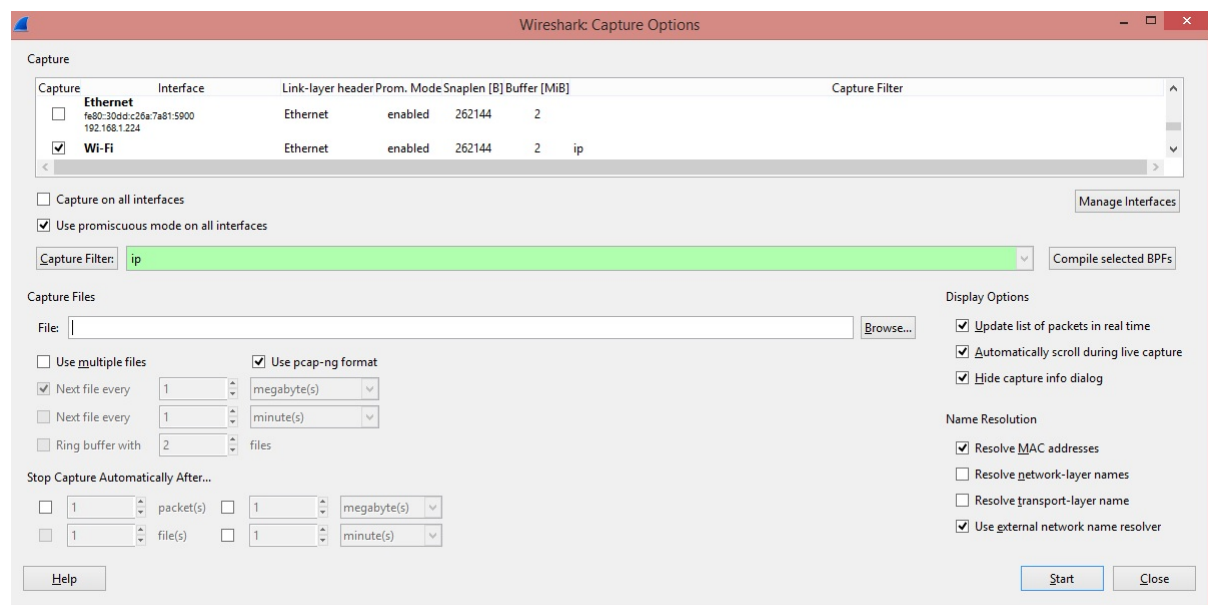
Bij het klikken op een specifieke bedreiging is er een gedetailleerde uitleg zichtbaar. Deze uitleg bevat o.a. een voorgestelde oplossing op het probleem en hyperlinks die verwijzen naar technische documenten die het probleem toelichten. Dit is enkel een simpel gebruik van de Nessus-tool, deze kan nog veel uitgebreider gebruikt worden, maar dit is in dit geval niet aan de orde. (Jackson, 2010)

4.5 Packet capture tools

Bij het uitvoeren van een risico-analyse mag er niet vanuit gegaan worden dat de IPS en Firewall zomaar werken zonder problemen. Deze zaken moeten grondig getest worden en dit kan gedaan worden via een packet capture tool. Volgens Jackson (2010) is Wireshark hiervoor de meest geschikte tool die elke persoon die een risico-analyse

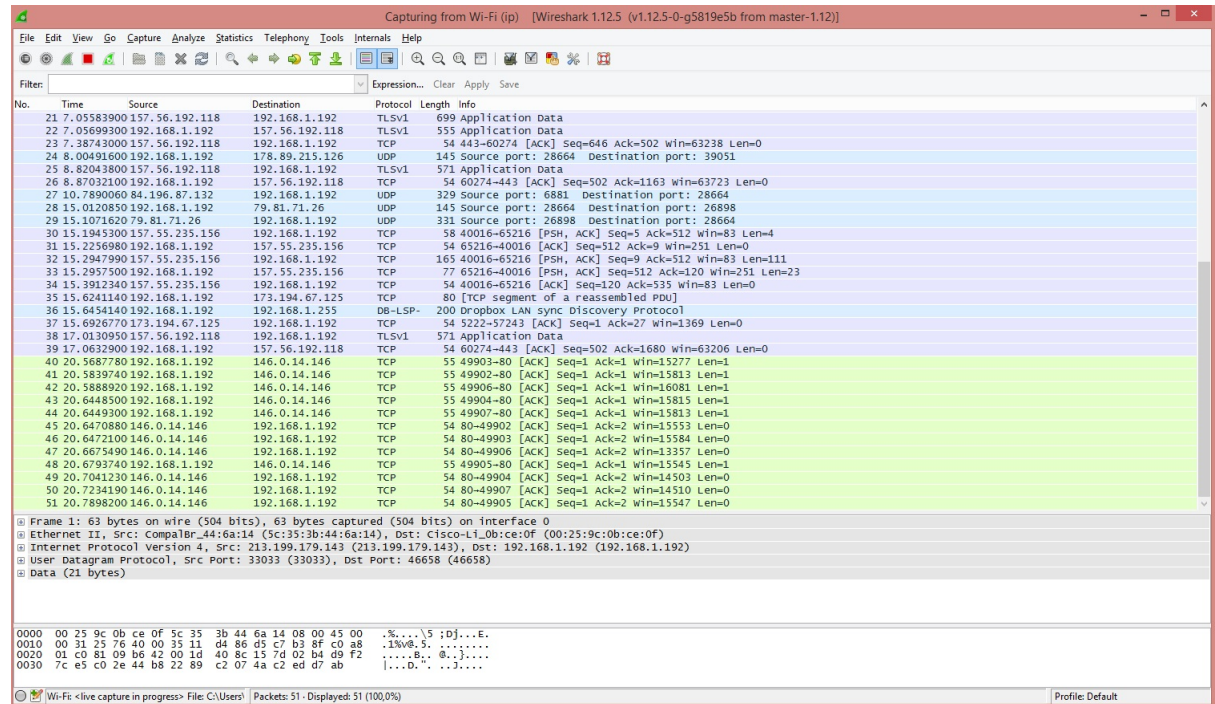
uitvoer moet kunnen gebruiken.

Wireshark slaat live verkeer op van de kabels, leest verkeer van een opgeslagen bericht en vertaalt honderden protocollen. Zijn gebruikersvriendelijke GUI zorgt ervoor dat het makkelijker te gebruiken is dan zijn concurrenten en geven ook een mooi overzicht van wat er al gedaan is en wat er nog moet gebeuren. Bij het opstarten van de applicatie kan er een direct een interface gekozen worden waar het verkeer van moet worden onderzocht. Bij het klikken op de startknop wordt er direct begonnen met de scan, maar in het „capture options”-scherm kan er verder gespecificeerd worden welk verkeer er precies moet worden bekeken.



Figuur 4.2: Voorbeeld van Wireshark-opties

Bij het drukken op start komt er een scherm tevoorschijn waar er alle specifieke pakketten waar naar zijn gevraagd zichtbaar worden. In dit geval is er gekozen om alle IP-pakketten van de wifi te onderzoeken. De kleurcode van de pakketten is ook belangrijk. Zo zijn groene pakketten TCP-verkeer, de blauwe zijn DNS, licht blauw is UDP-verkeer en zwart zijn TCP-pakketten met problemen. Deze kleuren kunnen natuurlijk naar eigen voorkeur ingesteld worden. (Hoffman, 2014)



Figuur 4.3: Voorbeeld van Wireshark-scan op wifi

Voor een auditor is dit zeer handig omdat er specifieke „captures” kunnen opgeslagen en bekeken worden. Deze captures kunnen ook opnieuw worden gedraaid door een netwerkinterface op bijvoorbeeld een willekeurige laptop om beveiligingstesten uit te voeren. Zo kan er gekeken worden per applicatie, per specifieke soort pakketten waar er eventuele beveiligingsproblemen zijn. Bij het dubbelklikken op een pakket kan er ook gekeken worden naar verdere details.

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 uitgeprobeerd. 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 netwerkbeheerders 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 ingetyped: „*hydra -t 1 -l BaeleAdministrator -P /root/woordenlijst.txt. -vV <IP-ADRES slacht-offer> ftp*”. Daarna wordt elk woord in de lijst apart uitgeprobeerd 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 platgegooid 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.

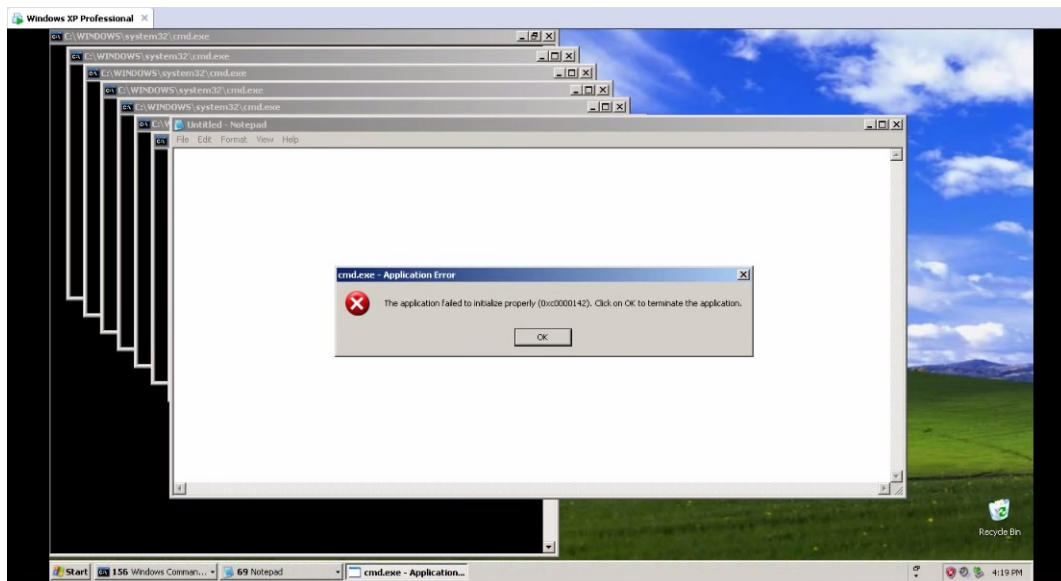
5.3 Netwerklaag

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 ververst. 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

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>.

Cisco (2013). *SQL Injection*. 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>.

Gibson, D. (2011). *Exploring common web server attacks*. <http://www.pearsonitcertification.com/articles/article.aspx?p=1713591>.

Hoffman, C. (2014). *how to use wireshark to capture filter and inspect packets*. <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>.

Jackson, C. (2010). *Network security auditing*. ciscopress.

Messer, J. (2007). *Secrets of Network Cartography: A Comprehensive Guide to nmap*. Professor Messer, 2 edition.

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.

- Nuckolls, J. (2011). *Create ASP.Net web app and SQL server database*. 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/>.
- Siddharth, S. (2006). *Five common web application vulnerabilities*. <http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities>.
- Stanek, W. R. (2009). *Windows Server 2008 Administrator's pocket cons*. Microsoft, 2de editie edition. <https://technet.microsoft.com/en-us/magazine/ff741764.aspx>.
- 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
4.1	Voorbeeld Nessus-scan (Bron: http://soft365.vn)	20
4.2	Voorbeeld van Wireshark-opties	21
4.3	Voorbeeld van Wireshark-scan op wifi	22
5.1	Voorbeeld Malware-aanval	28

Lijst van tabellen