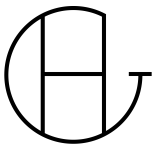

HoGent

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 hoor je regelmatig eens in het nieuws dat er een bedrijf is opgelicht door professionele hackers, oplichters die zijn binnen gedrongen in hun netwerk en gevoelige informatie hebben gebruikt om zaken te verkrijgen. 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.

Mijn grootste doelstelling is om een overzicht te voorzien van welke soorten maatregelen er zeker moeten getroffen worden om een netwerk optimaal te beveiligen. Dit gaande van de router tot de switch tot de server. Ik wil zelf ook zo een beveiligd netwerk/server kunnen opzetten en zelf kunnen testen dat er geen enkele vorm van bekende bedreigingen binnen kan. Tot slot wil ik te weten komen of er in het bedrijfsleven wel nood en budget is voor zulke hevige beveiligingen.

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 je router en switch zo optimaal mogelijk beveiligd? Hoe wordt de server zo goed mogelijk beveiligd? Wat zijn de voor -en nadelen van bepaalde beveiligingstechnieken?

Zijn de 'best practices' voldoende als beveiliging tegen een externe of interne aanval? Wat is de beste manier om als administrator sporen terug te vinden van een aanval? (KAN NOG VERANDEREN)

Voorwoord

Deze scriptie zou niet to stand gekomen zijn zonder de hulp van mijn stagementor en co-promotor Selami Top. Ik mocht gebruik maken van zijn huidig netwerk en ik mocht enkele zaken uitproberen op zijn nieuw netwerk. Hierdoor kon ik de zaken die ik onderzocht en opgezocht had uit proberen in een echte omgeving en kreeg ik een betere kijk op een realistische beveiliging. Verder wil ik ook mijn promotor Bert Van Vreckem bedanken die mij heeft geholpen om deze bachelorproef tot stand te brengen. Zijn tips en technische kennis waren een enorme hulp om dit resultaat te bekomen. (NOG WAT TOEVOEGEN). Tot slot wil ik alle auteurs bedanken van de lectuur die ik heb gebruikt om deze scriptie te maken (LIJST VAN ALLE AUTEURS?)

Inhoudsopgave

Hoofdstuk 1

Inleiding

De inleiding moet de lezer alle nodige informatie verschaffen om het onderwerp te begrijpen zonder nog externe werken te moeten raadplegen (**?**). Dit is een doorlopende tekst die gebaseerd is op al wat je over het onderwerp gelezen hebt (literatuuronderzoek).

Je verwijst bij elke bewering die je doet, vakterm die je introduceert, enz. naar je bronnen. In LaTeX kan dat met het commando `\cite{}` of `\citep{}`. Als argument van het commando geef je de "sleutel" van een "record" in een bibliografische databank in het BibTeX-formaat (een tekstbestand). Als je expliciet naar de auteur verwijst in de zin, gebruik je `\cite{}`. Soms wil je de auteur niet expliciet vernoemen, dan gebruik je `\citep{}`. Hieronder een voorbeeld van elk.

? schreef een van de standaardwerken over sorteer- en zoekalgoritmen. Experten zijn het erover eens dat cloud computing een interessante opportuniteit vormen, zowel voor gebruikers als voor dienstverleners op vlak van informatietechnologie (**?**).

1.1 Probleemstelling en Onderzoeksvragen

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

Port scanning is een bekende manier om iemand zijn netwerk in kaart te brengen en te kijken naar een manier hoe je er binnen kan geraken. Port scanning is kan jouw netwerk in gevaar brengen, maar kan er ook voor zorgen dat jouw netwerk beter beveiligd is als je weet hoe je het moet gebruiken en hoe je jezelf ertegen moet beschermen. De vraag die hier wordt gesteld is hoe dat je port scanning als ethische hacker kan gebruiken om jouw netwerk beter te beveiligen tegen mensen die port scannen gebruiken voor niet zo ethische doelstellingen.

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 je als netwerkbeheerder dit direct of toch zo snel mogelijk wilt te weten komen. Als er een aanval gaande is dan is het belangrijk dat je dit snel weet en dat je snel de oorzaak vindt en weet wat er precies aan het gebeuren is. Hetzelfde geldt voor wanener er een aanval heeft plaatsgevonden in de geschiedenis. Als administrator is het jouw taak om dit makkelijk op te sporen en ervoor te zorgen dat dit in de toekomst niet meer gebeurd.

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 webserver met ASP.net-applicatie draaiende als slachtoffer, één Kali Linux-machine als aanvaller en één Windows 8.1-machine die als client fungeert. De twee Windows-machines moeten geconfigureerd worden volgens best practice-beveilging.
3. 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 het betreft een externe aanval. Er wordt een lijst gemaakt met welke aanvallen er gaan gedaan worden en welke succesvol worden uitgevoerd en welke falen. Indien een aanvaal succesvol wordt uitgevoerd, dan zullen de best practices moeten aangevuld worden.
4. Het uitvoeren van een post-mortem om sporen van inbraak bloot te leggen en kijken waar het probleem zich bevindt.

2.1 Voorkennis en onderzoek

Voordat er kan worden begonnen aan dit onderzoek, is er een goede tot zeer goede kennis vereist over de volgende onderwerpen:

- Het installeren en configureren van Windows Server 2012 R2 met de volgende rollen aanwezig: Active Directory Domain Services, DHCP, DNS, IIS, ...
- Het opzetten van een ASP.net applicatie in IIS 8 met een achterliggende databank.
- Basiskennis over Microsoft SQL Manager of een andere databank software.
- Kennis over Kali Linux.
- Kunnen werken met Linux en Windows command prompt.
- Degelijke kennis over security met in het bijzondere penetratietestingtools zoals .....
- Controle overnemen van pc zonder firewall.

In de bibliografie staat een uitgebreide lijst met schriftelijke en digitale boeken en talrijke websites die gebruikt zijn bij het schrijven van dit onderzoek en dan ook ervoor zorgen dat bovenstaande vereisten voldaan zijn voordat er wordt begonnen aan het echte werk.

2.2 Opzetten testomgeving

2.2.1 Installatie + configuratie server

De Windows Server 2012 R2-virtuele machine is de eerste die moet worden opgezet. Er wordt gebruik gemaakt van VMWare Workstation en hierin wordt er een nieuwe virtuele machine aangemaakt met 60GB ruimte die dynamisch gealloceerd wordt en twee netwerkadapters. Nadat Windows Server 2012 R2 is geïnstalleerd wordt de naam van de server verandert naar "WebServerën deze zal hierdoor ook aangesproken worden in het verdere onderzoek. De eerste rol die wordt geïnstalleerd is de rol textitActive Directory Domain Services. Daarna wordt de WebServer domeincontroller gemaakt in het fictieve domein "Baele.be".

Op de server zijn 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 networkën 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.

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 lookupëen zone aangemaakt met de naam "1.168.192.in-addr.arpaën 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 router is de server zelf dus het IP-adres is 192.168.1.2 net als de DNS-server. Tot slot wordt de scope geactiveerd.

Aangezien deze server een webserver is, zal de IIS-rol met al zijn features ook worden geïnstalleerd. .....

2.2.2 Opzetten testomgeving

Om zelf wat ervaring op te doen met port scanning ben ik gestart met een virtuele machine te maken waarop Windows Server 2012 R2 op geïnstalleerd staat en deze heb ik de naam **ADServer** genoemd. Als eerste heb ik deze domeincontroller gemaakt in het fictieve domein *Baele.be*. Verder heb ik ook de rollen DNS, DHCP en Externe toegang geïnstalleerd en heb ik als subnet gekozen voor 192.168.1.0/24 waar ik de range 192.168.1.1 tot 192.168.1.30 heb ik uitgesloten voor distributie. Dan ben ik naar de website gegaan van Microsoft om SQL server 2012 te downloaden en te installeren. Ook heb ik de rol IIS 8 geïnstalleerd en heb ik een kleine lokale website gemaakt met een ASP.NET-applicatie op, deze is te bereiken via "*baele.be*". Deze applicatie heb ik gemaakt via Microsoft Visual studio en heeft ook een SQL-databank in de backend. Op de startpagina worden namen weergegeven die in een tabel in de databank zitten. Je kan je ook inloggen via een naam en wachtwoord die zich in de databank bevinden. Als je bent ingelogged dan kan je een speciale pagina "member"bekijken en als je niet ingelogged bent dan lukt dit niet. Tot slot heb ik de server het IP-adres 192.168.1.2 gegeven. Deze zaken moeten zich allemaal op de server bevinden zodat ik mijn onderzoeksvraag goed kan beantwoorden.

Nu dat er 1 server opstaat is het tijd om enkele hosts op te zetten en deze toe te voegen aan het domein. Ik heb 3 Windows hosts opgezet met de IP-adressen 192.168.1.31 - 192.168.1.32 - 192.168.1.33 en naam WS1 - WS2 - WS3. WS1 is een Windows 8.1-machine, WS2 is een Windows 7-machine en WS1 is een Windows Vista-machine. Tot slot heb ik een kali virtuele machine gemaakt om in het netwerk binnen te dringen. Met deze 5 virtuele machines kan ik verschillende soorten software en technologieën testen die ervoor zorgen dat ik mijn onderzoeksvragen zo nauwkeurig en correct mogelijk kan beantwoorden.

2.2.3

Hoofdstuk 3

Opzetten server met best practises beveiliging

´

3.1 Inloggen

Eén van de eerste zaken dat moet gebeuren is het uitschakelen van de inlognaam "Administratorën 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-accountën 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 "BaeleAdministratorën is deze lid geworden van de groepen *Administrators, Domeinadministrators en domeinconctrollers*.

3.2 Updates

Nog een belangrijke onderdeel van een server met best practice beveiliging, is het constant downloaden en installeren van updates. Het is dan ook aanbevolen dat je de updates automatisch laat uitvoeren. Dit zorgt ervoor dat de server continu is voorzien van de beste beveiliging en dat alle bugs die er op die moment aanwezig zijn, zijn verdwenen.

3.3 Firewall

Default is de firewall al vrij goed beveiligd tegen de meeste zaken. Er is echter één aanpassing die in de praktijk veel wordt toegepast en die ook door velen 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 doe je 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". Voor de rest zijn er geen algemene best practices te vinden voor de Firewall.

3.4 IIS

3.4.1 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.

3.4.2 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 gebeurd 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 äanvraagfilteringën naar het tabblad "HTTP-termen"te gaan. Hier wordt als actie gekozen "Term weigeren...ën wordt "OPTIONSïngevuld en op OK gedrukt. Nu staat deze regel als enigste in de lijst en is deze best practice in orde gebracht.

3.4.3 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.

3.4.4 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.

Hoofdstuk 4

Aanvallen webserver

Hoofdstuk 5

Post mortem

Hoofdstuk 6

Notities

Hier hou ik de zaken bij die ik al heb uitgetest, maar die ik nog niet bij 1 van de 3 hoofdstukken heb geplaatst. Dit is mijn tijdelijke "dump"waar ik test zaken schrijf voor de bij de echte hoofdstukken terecht komen.

6.1 Sockstress DDOS-aanval

6.1.1 Uitvoering en schade

Het vastlopen van een server kan op verschillende manieren. De eerste manier die ik heb geprobeerd om de webserver te laten vastlopen is *sockstress*. Dit is een methode die wordt gebruikt om servers over het internet aan te vallen gebruik makende van TCP. Deze methode zorgt ervoor dat het lokale geheugen zoveel aanvragen moet behandelen dat deze langzaam maar zeker helemaal volloopt totdat de server is vastgelopen en de server is gecrashed. Je kan dit ook een DOS (Denial of Service)-aanval noemen. De manier om dit uit te testen is door twee virtuele machines erbij te nemen. Langs de ene kant nemen we de slachtoffermachine, namelijk de Windows Server 2012 R2 webserver-virtuele machine genaamd ADServer, en langs de andere kant de aanvaller, de Kali Linux-machine. De ADServer heeft een standaard Firewall die geen extra configuratie heeft gekregen.

Op de aanvallersmachine gaan we naar de command line en geven we deze lijn code in *'nmap <ipadres slachtoffer>'* en we schrijven alle poorten op die we te zien krijgen. Wat er hier gebeurd is dat we kijken welke poorten er open zijn en kunnen worden aangevallen. Daarna openen we een apart terminalvenster en laten we daar een gedownload script draaien genaamd *"./arppoi"*. In dat scriptje hoef je het geschreven MAC-adres enkel te veranderen naar het MAC-adres van de aanvaller en daarna kan je het scriptje uitvoeren dat zorgt voor ARP spoofing. Nadat dit is gedaan hoef je enkel in het andere terminalvenster dit lijntje in te voeren: *"./sockstress -A -C -1 -d <IP van target> -m -1 -Ms -p <alle opgeschreven poorten> -r 100000 -s 172.16.246.0/25 -vv"* om de aanval te starten. Als je deze zaken hebt uitgevoerd, dan kan je kijken naar hoeveel RAM er wordt gebruikt op de server en dan zie je dat dit exponentieel aan het stijgen is tot dat deze het maximum bereikt en de server is vastgelopen. Daarna kan je de server enkel nog aan de praat krijgen door deze manueel uit te zetten via de aan/uit-knop en dan weer op te starten. Dit zorgt ervoor dat de server onbereikbaar is tot dit gebeurd en dat de bijhorende webserver onbeschikbaar is tot er een reboot komt. Het spreekt voor zich dat deze aanval.

6.1.2 Bescherming en preventie

Op papier heb ik al 1 oplossing, maar ik moet uitdokteren hoe ik dit kan testen en ik moet nog research doen naar meerdere mogelijkheden.

Hoofdstuk 7

Conclusie

Curabitur nunc magna, posuere eget, venenatis eu, vehicula ac, velit. Aenean ornare, massa a accumsan pulvinar, quam lorem laoreet purus, eu sodales magna risus molestie lorem. Nunc erat velit, hendrerit quis, malesuada ut, aliquam vitae, wisi. Sed posuere. Suspendisse ipsum arcu, scelerisque nec, aliquam eu, molestie tincidunt, justo. Phasellus iaculis. Sed posuere lorem non ipsum. Pellentesque dapibus. Suspendisse quam libero, laoreet a, tincidunt eget, consequat at, est. Nullam ut lectus non enim consequat facilisis. Mauris leo. Quisque pede ligula, auctor vel, pellentesque vel, posuere id, turpis. Cras ipsum sem, cursus et, facilisis ut, tempus euismod, quam. Suspendisse tristique dolor eu orci. Mauris mattis. Aenean semper. Vivamus tortor magna, facilisis id, varius mattis, hendrerit in, justo. Integer purus.

Vivamus adipiscing. Curabitur imperdiet tempus turpis. Vivamus sapien dolor, congue venenatis, euismod eget, porta rhoncus, magna. Proin condimentum pretium enim. Fusce fringilla, libero et venenatis facilisis, eros enim cursus arcu, vitae facilisis odio augue vitae orci. Aliquam varius nibh ut odio. Sed condimentum condimentum nunc. Pellentesque eget massa. Pellentesque quis mauris. Donec ut ligula ac pede pulvinar lobortis. Pellentesque euismod. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent elit. Ut laoreet ornare est. Phasellus gravida vulputate nulla. Donec sit amet arcu ut sem tempor malesuada. Praesent hendrerit augue in urna. Proin enim ante, ornare vel, consequat ut, blandit in, justo. Donec felis elit, dignissim sed, sagittis ut, ullamcorper a, nulla. Aenean pharetra vulputate odio.

Quisque enim. Proin velit neque, tristique eu, eleifend eget, vestibulum nec, lacus. Vivamus odio. Duis odio urna, vehicula in, elementum aliquam, aliquet laoreet, tellus. Sed velit. Sed vel mi ac elit aliquet interdum. Etiam sapien neque, convallis et, aliquet vel, auctor non, arcu. Aliquam suscipit aliquam lectus. Proin tincidunt magna sed wisi. Integer blandit lacus ut lorem. Sed luctus justo sed enim.

Morbi malesuada hendrerit dui. Nunc mauris leo, dapibus sit amet, vestibulum et, commodo id, est. Pellentesque purus. Pellentesque tristique, nunc ac pulvinar

adipiscing, justo eros consequat lectus, sit amet posuere lectus neque vel augue. Cras consectetuer libero ac eros. Ut eget massa. Fusce sit amet enim eleifend sem dictum auctor. In eget risus luctus wisi convallis pulvinar. Vivamus sapien risus, tempor in, viverra in, aliquet pellentesque, eros. Aliquam euismod libero a sem.

Nunc velit augue, scelerisque dignissim, lobortis et, aliquam in, risus. In eu eros. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Curabitur vulputate elit viverra augue. Mauris fringilla, tortor sit amet malesuada mollis, sapien mi dapibus odio, ac imperdiet ligula enim eget nisl. Quisque vitae pede a pede aliquet suscipit. Phasellus tellus pede, viverra vestibulum, gravida id, laoreet in, justo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Integer commodo luctus lectus. Mauris justo. Duis varius eros. Sed quam. Cras lacus eros, rutrum eget, varius quis, convallis iaculis, velit. Mauris imperdiet, metus at tristique venenatis, purus neque pellentesque mauris, a ultrices elit lacus nec tortor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent malesuada. Nam lacus lectus, auctor sit amet, malesuada vel, elementum eget, metus. Duis neque pede, facilisis eget, egestas elementum, nonummy id, neque.

Lijst van figuren

Lijst van tabellen