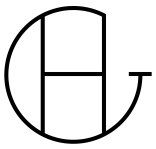


HoGent

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 beveilgings 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 beveilgde 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, video-lessen, ... die ik heb gelezen. Dankzij hun bijdrage is de kwaliteit van deze scriptie en mijn kennis enorm verbeterd.

Inhoudsopgave

Hoofdstuk 1

Inleiding

In deze scriptie zal een fictief netwerk opgezet worden dat een domeincontroller en een webserver zal bevatten. Deze webserver is uiteraard lid van hetzelfde netwel als de domeincontroller en beiden zijn verbonden aan dezelfde switch en deze switch is op zich dan verbonden met een router die dan op zijn beurt verbonden is met het internet.

Het is de bedoeling dat er met een hackermachine zal geprobeerd worden om de webserver te kraken op een paar manieren en deze webserver moet deze aanvallen overleven. De bekendste en meest voorkomende aanvallen zullen uitgevoerd worden tegen deze webserver en het is de bedoeling dat de eerder geïmplementeerde best practices voldoende zijn om de server te beschermen tegen deze aanvallen. Is dit niet het geval dan zullen de best practices moeten aangevuld worden.

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?

Er circuleren talrijke zogenaamde „best practices" om een webserver te beveiligen tegen interne en externe bedreigingen. Deze best practices worden geïmplementeerd op een webserver en daarna wordt deze aangevallen door enkele veelgebruikte en bekende interne en externe aanvallen om te testen of deze wel effectief genoeg zijn. Indien dit niet het geval is wordt er gekeken naar hoe deze het beste worden aangevuld.

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.

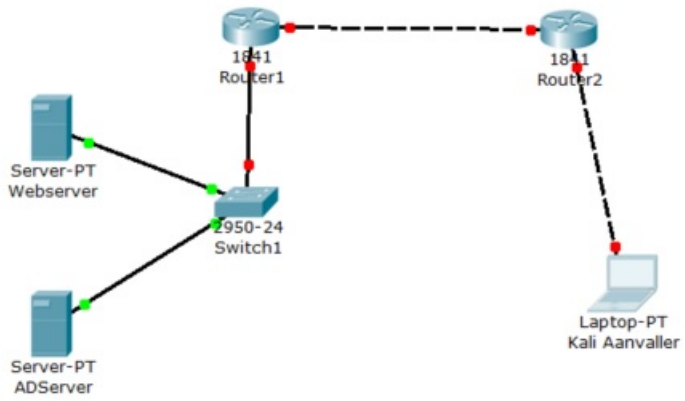
Hoofdstuk 2

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 waar er eventuele gaten zijn in het netwerk en deze dan dichten.
4. Met behulp van penetration testing tools beveiligingsproblemen zoeken en uitbuiten. Hier wordt er vanuit gegaan dat er wel en geen fysieke toegang is tot de server dus het betreft zowel interne als externe aanvallen. 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.

In de afbeelding 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



Figuur 2.1: Proefopstelling

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.

2.0.3 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 twee netwerkadapters 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 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 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.

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 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.

2.0.4 Installatie + configuratie WebServer

De installatie start op dezelfde manier als de voorgaande machine, maar in dit geval wordt de machine „WebServer" genoemd. Deze server wordt ook lid gemaakt van het domein „Baele.be". Op deze server is het belangrijk dat de rol ....

2.0.5 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 en 512MB aan RAM-geheugen. Bij het starten van de installatie is het gemakkelijk dat er gekozen wordt voor „graphical install". De meeste stappen zijn voor de hand liggend, maar bij partition disks wordt er 'guided-use entire disk' het best geselecteerd. Voor de rest zijn de overige stappen niet zo belangrijk en is de installatie zo afgerond.

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-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 gebruik 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.

3.2 Updates

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

3.3 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 gebeurd 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 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.

3.5 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 voldoen. 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.

3.6 IIS

3.6.1 Plaatsing

De plaatsing van IIS is belangrijk. 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 beveiligingsmogelijkeden 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.

3.6.2 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)

3.6.3 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.

3.6.4 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 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 „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 enigste in de lijst en is deze best practice in orde gebracht.

3.6.5 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.

3.6.6 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 gebeurd 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.

3.6.7 Inschakkelen 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 slecteren en op logging te klikken. Best wordt er gekozen om een nieuw bestand aan te maken want deze bestanden groeien vrij snel.

Hoofdstuk 4

Risico-analyse

Bij een risico-analyse wordt een netwerk helemaal onder de loep genomen en wordt er gekeken en gezocht naar alle mogelijke gevaren die een netwerk kan ondergaan van zowel mensen als de natuur en zowel intern als extern. Voordat een nieuw geplaatst netwerk in het bedrijf wordt gebruikt, is het best dat er eerst een risico-analyse plaats vindt om te kijken waardat er nog problemen kunnen zijn en waar dat er nog wat verscherping van de beveiling nodig is.

4.1 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 grotes 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 acief 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.

4.2 Kwestbaarheidscanner

Nessus is volgens Jackson (2010) een populaire kwetsbaarheidscanner die zoekt naar zwakke plekken in besturingssystemen, netwerkapparaten 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 toepassing zijn om het te onderzoeken netwerk. 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)

Figuur 4.1: Voorbeeld Nessus-scan

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 slachtoffer> ftp*". Daarna wordt elk woord in de lijst apart uitgeprobeerd totdat er een juiste combinatie is of tot de lijst doorlopen is. (Moon, Mei)

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 gebeurd 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 bedoelt 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.

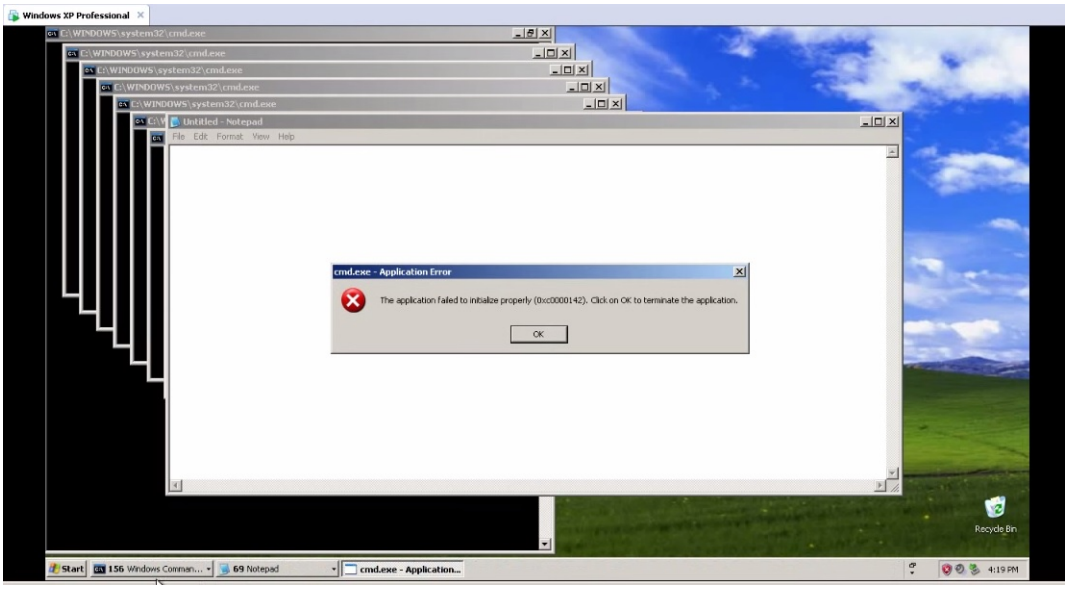
5.3 Netwerklaag

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 gebeurd wordt er ook een nieuwe kladblokapplicatie geopend. Dit gebeurd 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.

5.3.2 Keylogger

Nog uitwerken

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" ingestyped 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 prestatiemeter-tool kunnen bepaalde zaken makkelijk in de gaten gehouden worden. In de prestatiemeter 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 „prestatiemeter" 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 gedubelklikt 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 paramters 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 aangemaakt 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 dubbeklikken alle paramters 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.

6.2.2 Polymon

Nog uitwerken

Hoofdstuk 7

Conclusie

Bibliografie

Angus, C. (2005). *SQL Injection and some tips on how to prevent them*.

Cisco (2013). *SQL Injection*.

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*.

Moir, R. (2003). Defining malware. *Microsoft technet*.

Moon, S. (Mei). *Crack ftp passwords with Hydra*.

Nabors, E. (2013). *Managing the Windows Server 2012 Firewall*.

Wilde, B. (2013). *Hacking Tutorial: Brute Force Password Cracking*.

Lijst van figuren

Lijst van tabellen