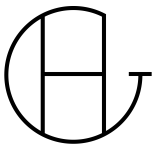

HoGent

Faculteit Bedrijf en Organisatie

De efficiëntste manier om een Windows Server 2012 R2 netwerk te beveiligen tegen interne en externe bedreigingen in het bedrijfsleven

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

De efficiëntste manier om een Windows Server 2012 R2 netwerk te beveiligen tegen interne en externe bedreigingen in het bedrijfsleven

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?

- Wat zijn de bekendste soorten van externe bedreigingen en hoe los je deze het efficiëntst op? - Wat zijn de bekendste soorten van interne bedreigingen en hoe los je deze het efficiëntst op? - Is er in het huidige bedrijfsleven (kleine, middelgrote en grote ondernemingen) nood/budget aan een stevige beveiliging. - Hoe beveilig je de router en switch zo optimaal mogelijk? - Hoe beveilig je de server en werkstations zo optimaal mogelijk? - Wat zijn de voor -en nadelen van bepaalde beveiligingstechnieken? .... (KAN NOG VERANDEREN)

Voorwoord

Deze scriptie zou niet to stand gekomen zijn zonder de hulp van mijn stagementer 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. (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 Hoe kan port scanning de beveiliging van je eigen netwerk verbeteren en wat zijn de gevaren ervan?

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 en efficiënste manier om jouw netwerk te beschermen tegen port scanning?

Hoofdstuk 2

Methodologie

2.1 Port scanning

2.1.1 Onderzoek

Om een goed antwoord te kunnen geven op deze onderzoeksvraag moet ik eerst een goede kennis hebben over het onderwerp. Dit heb ik gedaan door het verzamelen van lectuur over hoe je moet ethisch hacken en wat port scanning precies is. Om de gevaren van port scanning te kennen, moet ik eerst weten hoe een port scan werkt en hoe ik de output ervan kan interpreteren.

2.1.2 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. Als eerste heb ik deze domeincontroller gemaakt in het fictieve domein *HARDO*. Verder heb ik ook de rollen DNS, DHCP en Externe toegang geïnstalleerd en heb ik al 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. Daarna ben ik naar de website van nmap gegaan om de nmap-tools te downloaden. Deze zijn zeer belangrijk om zelf aan port scanning te doen. Tot slot heb ik de server het IP-adres 192.168.1.2 gegeven.

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 8.1-hosts opgezet met de IP-adressen 192.168.1.31 - 192.168.1.32 - 192.168.1.33 en naam WS1 - WS2 - WS3. Met deze 4 virtuele machines kan ik verschillende soorten software en technologieën testen die ervoor zorgen dat ik mijn onderzoeksvragen zo nauwkeurig en correct mogelijk kan beantwoorden.

2.1.3

Hoofdstuk 3

Port scanning interpreteren

3.1 Wat is port scanning?

Om te antwoorden op de onderzoeksvragen moet je eerst weten wat port scanning precies is en doet. Port scanning is één van de meest gebruikte en bekendste manieren die er bestaat om een weg te vinden in het netwerk van een persoon of een bedrijf. Bij een port scan wordt er gekeken welke poorten er allemaal open staan in een netwerk. Via poorten wordt er informatie verzonden en ontvangen dus je kan deze techniek vergelijken met in een gang met 65 535 deuren aan elke deur eens voelen en kijken of deze open staat of gesloten is.

Door een port scan uit te voeren op een netwerk kan je zien welke poorten er open zijn, maar ook welke poorten er luisteren. Dit wilt zeggen welke poorten er informatie ontvangen. Je kan ook zien welke beveiligings apparaten zoals firewalls die aanwezig zijn tussen de zender en de ontvanger. Deze techniek wordt ook wel fingerprinting genoemd en wordt vaak gebruikt door aanvallers om een zwak punt in het netwerk te vinden.

3.2 Soorten port scans MEER INFO ZOEKEN

Er zijn verschillende soorten port scans en elk van deze hebben hun eigen accenten.

- Vanilla = Ook wel een "full scan"genoemd. Hierbij wordt er geprobeerd om met alle 65 535 poorten verbinding te maken. Er wordt een SYN flag (vraag om te verbinden) verzonden en na het ontvangen van een SYN-ACK respons wordt er een ACK flag teruggestuurd. Dit staat ook wel bekend als een TCP handshake. Deze soort scans zijn zeer nauwkeurig maar zijn makkelijk detecteerbaar omdat deze soort verbindingen altijd worden gelogged door de firewall.

- Fragmented Packets = De scanner zend fragmenten van pakketten uit die door een simpele packet filter geraken in een firewall.
- Strobe = Is een iets specifiekere scan die enkel kijkt naar bekende services die kunnen geexploid worden.
- Stealth scan = De scanner blokkeert de gescande computer om de port scan activiteiten te onthouden
- UDP = Er wordt gekeken naar open UDP-poorten.
- FTP Bounce = Scanner gaat door een FTP-server om de bron van de scan te verbergen.

Hoofdstuk 4

Port scanning als bedreiging

Hoofdstuk 5

Port scanning als hulpmiddel

Hoofdstuk 6

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