Risico analyse

# Applicatielaag

Applicatie laag DDOS-aanvallen $https://conference.apnic.net/data/37/l7ddos\_apricot\_1393257782.pdf$

$https://www.youtube.com/watch?v=BYKnBki2WTc$

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 unavailble $https://www.youtube.com/watch?v=k1o9Ya8qxlU$ $https://code.google.com/p/r-u-dead-yet/$

XerXes DOs, lokale host maakt aanvalt en is anoniem en geen firewall kan beveiligen $http://www.securitytube.net/video/7530$

SQL Injectie = $https://www.acunetix.com/websitesecurity/sql-injection/$

http://hakipedia.com/index.php/SQL\_Injection

Telnet = https://www.youtube.com/watch?v=KUyUICumTRA

# Transportlaag

Aanvallen tegen TLS/SSL = voorbeeld $http://en.wikipedia.org/wiki/Transport\_Layer\_Security$

TCP flooding = $http://searchsecurity.techtarget.com/definition/SYN-flooding$ $https://samsclass.info/123/proj10/sockstress.htm$

Sockstress = $https://www.youtube.com/watch?v=hKj\_Dwyt0a0$

port scanning = $http://www.garykessler.net/library/is\_tools\_scan.html$  
🡪 oplossing: http://en.wikipedia.org/wiki/Port\_knocking

# Internetlaag

Oplossing Ping flood = Since ICMP packets should be rare in a normal traffic situation, F5 BIG-IP Local Traffic Manager (LTM) and BIG-IP Advanced Firewall Manager (AFM) are able to mitigate ICMP floods by limiting the rate of all ICMP traffic, and then dropping all ICMP packets above this limit. BIG-IP LTM and BIG-IP AFM provide the ability to set a limit on the maximum number of ICMP packets to prevent the server from ever getting flooded.

$http://kalilinuxfans.blogspot.be/2013/06/hack-remote-computer-via-ip-and-open.html$

Ping flood (ICMP flood) = $http://ghostgrid.blog.com/2010/12/16/ping-flooding/$

ARP spoofing = voorbeeld $http://en.wikipedia.org/wiki/Network\_interface\_layer\_security$ Oplossing+toepassing = $http://www.veracode.com/security/arp-spoofing$ + $http://www.watchguard.com/infocenter/editorial/135324.asp$ + $http://en.wikipedia.org/wiki/ARP\_spoofing$ + $http://searchsecurity.techtarget.com/video/How-to-use-Wireshark-to-detect-and-prevent-ARP-spoofing$

Man in the middle = $http://securityxploded.com/art-of-arp-spoofing.php$

# Netwerktoeganglaag

VLAN attack

Keystroke logging = $https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/$ $http://searchsecurity.techtarget.com/tip/How-to-detect-and-prevent-keylogger-attacks$ $http://en.wikipedia.org/wiki/Keystroke\_logging$

SCANNERS TEKST

\section{Netwerkscanner}

\cite{Jackson2010} 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. \citep{Messer2007}. \newline

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.

\section{Kwestbaarheidscanner}

Nessus is volgens \cite{Jackson2010} 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. \newline

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. \newline

\begin{figure}[H]

\begin{center}

\includegraphics[scale=0.60]{img/Nessus1}

\end{center}

\caption{Voorbeeld Nessus-scan}

\end{figure}

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) \newline

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. \citep{Jackson2010}

\section{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 \cite{Jackson2010} is Wireshark hiervoor de meest geschikte tool die elke persoon die een risico-analyse uitvoerd moet kunnen gebruiken. \newline

Wireshark slaat live verkeer op van de kabels, leest verkeer van een opgeslagen bericht en vertaald 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 gespecifieerd worden welk verkeer er precies moet worden bekeken.

\begin{figure}[H]

\begin{center}

\includegraphics[scale=0.50]{img/Wireshark1}

\end{center}

\caption{Voorbeeld van Wireshark-opties}

\end{figure}

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 UPD-verkeer en zwart zijn TCP-pakketten met problemen. Deze kleuren kunnen natuurlijk naar eigen voorkeur ingesteld worden. \citep{Hoffm2014}

\begin{figure}[H]

\begin{center}

\includegraphics[scale=0.40]{img/Wireshark2}

\end{center}

\caption{Voorbeeld van Wireshark-scan op wifi}

\end{figure}

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.

LOG DINGEN

\chapter{Post mortem}

%Hier ga ik een aanval uitvoeren en ga ik kijken waar je dit precies kan terugvinden als administrator of waar je kan het kan zien als het aan het gebeuren is.

\section{Manueel}

\subsection{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.

\subsection{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"'. \newline

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.

\subsection{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.

\section{Automatisch}

\subsection{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.

\subsubsection{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. \newline

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.

\subsubsection{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.