Erledigt Ossec auf Hack installieren...?

Beitrag von „variousos“ vom 30. März 2015, 11:12

Hallo an Alle,

ich würde gerne auf meinem Hack das OpenSouce Intrusion Detection System "Ossec" installieren. Meinen Cisco-Switch habe ich damit bereits ausgestattet und damit die Windowswelt- als auch BSD-Welt "abgesichert". Da es das System auch für den Mac gibt, hier die Frage ob das schon jemand installiert hat?

Wäre für Anregungen dankbar...

LG

variousos

Beitrag von „Doe1John“ vom 30. März 2015, 13:12

Falls du einer der ersten bist, die das nutzen wollen, kannst du uns ja berichten, ob es auch auf dem MAC funktioniert.
VG Hobbit

Beitrag von „variousos“ vom 30. März 2015, 15:39

Hallo Hobbit,

ich werde über das was ich heraus bekomme und vielleicht weiteres hier berichten.

DANKE

variousos

Beitrag von „Doe1John“ vom 30. März 2015, 16:01

jepp, wir freuen uns drauf..... 

Beitrag von „variousos“ vom 30. März 2015, 19:21

Hallo,

also...ich habe das Intension Detection System "OSSEC" auf meinem Hack erfolgreich installiert . Es meldete mir auch per Mail schon die eine oder andere "Notification". Die Installation ist etwas "tricky".

Ich kann die Installationsschritte hier ENTWEDER Step-by-Step aufzeigen...ODER einfach ein wenig warten, bis ich wirklich einen Nutzen daraus ziehen kann. Man liest viel Gutes über "OSSEC" (siehe letzte c´t).

Bitte um eine kurze Info zu meinem "ENTWEDER - ODER"... 

variousos

Beitrag von „al6042“ vom 30. März 2015, 19:24

Cool...

Danke schon mal für deinen Einsatz...
Ich würde gerne schon mal die Anleitung sehen und hier einen Thread zur Diskussion des Für und Widers begrüßen.

Beitrag von „variousos“ vom 31. März 2015, 16:53

Bei OSSEC handelt es sich um ein hostbasiertes Intrusion Detection System, dessen Aufgabe es ist, die Integrität des Systems sicherzustellen und Angriffe zu erkennen und abzuwehren und dem Nutzer auch zu melden.

Über die Notwendigkeit eines solchen Tools könnte man diskutieren. Ich setze es seit einiger Zeit in meiner Windows-Welt ein, sichere damit meine Domäne und auch sensible Bereiche wie die PKI und meinen Mailserver. In einigen Beiträgen von Administratoren wird sogar beschrieben, dass dies in Linux- und BSD-Systemen (wie MacOSX!) einen Virenscanner erübrigt. Aber das muss jeder selbst wissen!

Die Installation:

Zur Installation von OSSEC benötigen wir einen Compiler. Am einfachsten lässt sich das über das tool „Mac Ports“ reasisieren, welches es auch für Yosemite gibt.

Den Download von OSSEC, aktuell Version 2.8.1 können wir von der Seite http://www.ossec.net starten, anschließend entpacken.
Dann wechseln wir (meinst zu Downloads) in den dort befindlichen Ordner (ossec-hids-2.8.1) und führen im Terminal das Skript „install.sh“ aus.
Das mache ich einfach, in dem ich die ./install.sh ins Terminal ziehe. Bei mir musste ich das mit root-Rechten ausführen....also mit „sudo“.
Es werden dann einige Einstellungen abgefragt! Nach der Sprache, die man auf „de“ einstellen kann, wird nach demstart Modus gefragt. Will ich meinen Desktop absichern, wähle oder einen einzelnen Server, wähle ich „lokal“.
Bei „Server“ handelt es sich um das Management-Device für das gesamte Netzwerk, dass mit OSSEC überwacht werden soll. „Agent“ ist dazu gedacht, dass an einen zentralen Server gesendet wird. „Hybrid“ bedeutet, dass beide...Server und Agent installiert wird.

In meinem Fall habe ich „lokal“ gewählt!

Der vorgeschlagene Installationsort sollte man zustimmen (/var/ossec). Weiterhin wird nach einer email für Benachrichtigungen gefragt. Ich weiß offengestanden nicht, ob diese Auswahlmöglichkeit nur besteht, wenn man lokal einen eigenen Mailserver betreibt! Ich habe diese Möglichkeit allerdings genutzt.

Wenn die Installation beendet ist, muss das Programm gestartet werden!

Dies habe ich, um nicht so viel einzutippen wieder mit dem „reinziehen“ der entsprechenden Datei erledigt.
Diese liegt in /var/ossec/bin und heißt: „ossec-control“ (Bei mir musste ich zum öffnen der Ordner erst die Rechte vergeben). Dann starten wir mit mit dem Befehl:
„sudo /var/ossec/bin/ossec-control start“
Es erscheint daraufhin idealerweise:
Starting OSSEC HIDS v2.8 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.

So...das war erst einmal die Installation für OSSEC. Die grundsätzlichen Konfigaritionschritte habe ich ebenfalls aufgezeigt.

Ich sage unumwunden, dass das „Projekt IDS“ damit noch nicht beendet ist! Es gilt noch das Monitoring aufzuzeigen. Ich sammle gerade daraus meine Erfahrungen, was aber noch ein paar Tage in Anspruch nehmen wird.

Ich sollte hier in erster Linie ein Diskussiongrund liefern (wenn ich das richtig verstanden habe☺) über das Für- und Wider!

Ich freue mich auf entsprechende Beiträge. Wobei ich mich noch mehr über Erfahrungswerte oder Verbesserungsvorschläge freue.

DANKE

variousos

Beitrag von „al6042“ vom 31. März 2015, 17:07

Wow...

Vielen Dank für die Anleitung...

@Alle: Und los geht's! Was haltet ihr von der Möglichkeit mit diesem Produkt und der Nutzung von IDS (Intrusion-Detection-System) unter OSX oder grundsätzlich im privaten Bereich?

Beitrag von „Griven“ vom 2. April 2015, 21:36

> Zitat
>
> Started ossec-maild...

Sieht für mich so aus als wenn ossec einen eigenen mailerdeamon mitbringt sprich es den mailversand selbstständig regelt

---

Beitrag von „derHackfan“ vom 2. April 2015, 22:59

Ich dachte Ossec ist eine neue Version von Ozmosis, wenn ich aber Compiler lese, dann fühle ich mich wie ein Noob. :ziehharmonika:

Beitrag von „Griven“ vom 3. April 2015, 22:52

Nee OSSEC und Ozmosis haben mal so gar nichts miteinander zu tun