IOAs und IOCs

Laborufgabe Block 3

25HS

1 Aufgabenstellung

Mit Icinga2 (Eine Monitoring-Software) kann ganz einfach ein Skript aufgerufen werden. Das Skript muss eine ganz spezifische Ausgabe auf "stdout" aufweisen. Einmal eingebunden kann so etwas beliebiges überwacht werden.

Leider sprengt unser Stundenbudget die Möglichkeit eine komplette Icinga2-Instanz aufzusetzen (ca 2h), ein Service einzubinden (ca 30 Minuten) und ein Plugin zu schreiben (nochmals ca. eine Stunde). Wir Fokussieren uns deshalb primär auf den Teil mit dem Schreiben des Plugins. Optional können Sie natürlich alles machen, die Links zu allen Teilen sind unten unter den Hilfestellungen.

Plugins befinden sich je nach Distribution an verschiedenen Orten. Gängige Orte sind:

- /usr/lib/nagios/plugins
- /usr/lib64/nagios/plugins

Das Verzeichnis Nagios ist es deshalb, weil Icinga ursprünglich ein Fork mit komplett neugeschriebenem Core von Nagios ist. Der neue Core hat viele grosse Vorteile, weshalb heute typischerweise Icinga den Vorzug über Nagios gegeben wird.

Jetzt zur eigentlichen Aufgabe: Schreiben Sie zwei Plugins eines für IoAs. Das kann zum Beispiel ein Skript sein, dass die Fehlgeschlagenen SSH-Logins pro Benutzer prüft und ab einer bestimmten Schwelle (Idealerweise über Kommandozeilenparameter für "Warning" und "Critical" einstellbar) entsprechende Mitteilungen ausgibt. Das zweite Plugin soll als IoC root Logins zu ungewöhnlichen Zeiten melden (z.B. zwischen Mitternacht und drei Uhr Morgens).

Beide Plugins haben idealerweise Unterstützung für eine Hilfe, eine saubere Ausgabe, die Icinga/Nagios parsen kann, und die richtigen Exitcodes, damit das Plugin auch noch sauber funktioniert. Ein kleiner Hinweis: Monitoring sind typischerweise Zustands-basiert. Ein IDS aber eventbasiert. Wir verwenden hier ein Monitoring als IDS. Als Folge davon müssen wir uns Gedanken machen, ab wann wir ein IoA/IoC melden, und ab welchem Zeitpunkt wir die Meldung als "veraltet" verschwinden lassen. Im Idealen Fall können wir das ganze Stumm schalten (z.B. über ein Kontrollfile, das es uns erlaubt Alarme, die bekannt sind und bereits analysiert wurden zu quittieren). Auch dieser Teil ist natürlich optional. Im Moment ist es ausreichend, wenn Sie nur Alarme vom aktuellen Tag berücksichtigen. Dann können Sie einen Alarm nach Analyse für 24h quittieren im Monitoring (Das hat aber den Nachteil, dass subsequente Alarme am selben Tag ignoriert werden).

2 Hilfestellungen

- Wie man ein Plugin schreibt finden Sie unter `https://community.icinga.com/t/how-to-write-a-bash-script-wrapper-newbie-script-for-itl-check-yum-plugin/119`

- Ein Primer zum Aufsetzen von Icinga2 inklusive einiger Zusatzpakete, der einigermassen aktuell ist, finden Sie unter `http://www.netpingdevice.com/blog/primer-monitoringa-servernoj-komnaty-na-osnove-icinga-i-ustrojstv-netping`. Bitte beachten Sie, dass dieser Teil optional ist.
- Wie man ein eigenes Plugin als Service einbindet, finden Sie hier: `https://stevies blog.de/blog/en/2020/10/25/my-first-ever-icinga-plugin/`