Exposé

June 15, 2022

1 Motivation/Hintergrund

Sicherheit ist einer der, wenn nicht sogar der, zentralste Aspekt eines jeden It-Systems. Angesichts der Tatsache, das sowohl dass Internet bzw. ein gewisser Grad an Vernetzung verschiedener Geräte, als auch die Interaktion zwischen Mensch und Maschine einerseits nicht mehr wegzudenken sind und andererseits immer vielfältiger, dynamischer, schneller und öfter ablaufen ist Netzwerksicherheit integraler Bestandteil eines It-System . Kein PC, kein Laptop, kein Rechenzentrum, kein schlauer Ofen dieser Welt ist ohne das dazugehörige Netzwerk sonderlich brauchbar. Zugriffskontrolle ist wiederum ein zentraler Aspekt der Sicherheit eines Netzwerkes. Genauso wie IT-Systeme und unser Umgang mit ihnen dem Wandel der Zeit unterliegen, so müssen auch Entscheidungen wer, wann, wie, warum und worauf Zugriff erhält (oder eben nicht erhält) immer öfter, schneller, und besser getroffen werden. Da IDS, die ohne die Verwendung des vorhandenen Netzwerkkontextes Entscheidungen treffen, dieser Aufgabe nicht oder zumindest nicht ausreichend gewachsen sind, ist es dringend notwendig bereits vorhandene, noch ungenutzte Informationen in die Entscheidungsfindung eines jeden Netzwerk-Sicherheits-Monitoring mit einzubeziehen. Ebendiese bereits vorhandene Information die ich nutzen will ist Kontext.

2 Forschungsfrage/Herangehensweise

Wie in der Einleitung beschrieben ist das zentrale Ziel die Erhöhung der Netzwerksicherheit. Die Unterteilung in Forschungsfrage und Herangehensweise ist mir zum jetzigen Zeitpunkt ein wenig missglückt. Im Nachfolgenden habe ich dennoch versucht dieses Ziel in kleine und gut verständliche Teile zu zerlegen die möglichst wenig Interpretationsspielraum zulassen.

1. Verbesserung bestehender IDS-Lösungen(bessere/weniger Zugriffskontrollentscheidungen)

    1.1 Festlegung der IDS-Performancekriterien(bspw. Erkennungsrate/Rate der falsch-positiven Meldungen)

    1.2 Analyse des Ausmaßes der Mängel bestehender nicht-kontextsensitiver IDS-Systeme

1.3 Erläuterung der Notwendigkeit der Verwendung von Netzwerkkontext

2. Erstellung kontextsensitiver IDS-Signaturen

2.1 Definition eines Kontextbegriffs im Rahmen der Zugriffskontrolle

2.1.1 Historische Entwicklung des Kontextbegriffs

2.1.2 Darlegung/Erläuterung meiner Kontextdefinition

2.2 Kontextkategorisierung

2.2.1 Analyse bereits vorgeschlagener Kategorien

2.2.2 Erstellung einer Kontexttaxonomie

2.3 "Übersetzung"/Transfer der Taxonomie/Kategorien in IDS-Signaturen

2.3.1 Festlegung auf bestimmte IDS-Implementierungen

2.3.2 Analyse der IDS-Regel-Syntax

2.3.3 Abgleich zwischen Taxonomie und den in der Realität zur Verfügung stehenden Informationen

2.3.4 Umsetzung/Implementierung der Taxonomie in IDS-Signaturen

2.4 Test der kontextsensitiven Signaturen

2.4.1 (Auswahl eines bereits existierenden/ Erstellung eines eigenen) Datensatzes + dazugehörige Label

2.4.2 Aufbau eines oder mehrerer Netzwerke

2.4.1 Setup der verschiedenen IDS

2.4.2 Baseline mit non-kontextsensitiven Signaturen auf Datensatz

2.4.3 Test der kontextsensitiven Signaturen auf Datensatz

2.5 Auswertung der Testergebnisse

2.5.1 Vergleich der IDS-Alerts mit Datensatzlabeln

2.5.1.1 Baselineauswertung

2.5.1.2 Vergleich der Performance gemäß der in 1.1 festgelegten Kriterien zwischen non-kontextsenitiven und kontextsenitiven Signaturen

2.5.1.3 Vergleich der unterschiedlichen getesteten Kontextkategorie(kombinationen)

2.6 Konklussion

2.6.1 "Bewertung" der theoretischen Mächtigkeit einzelner Kategorien

2.6.2 Beurteilung/Einschätzung der tatsächlichen Verfügbarkeit von Kontext im Netzwerk

2.6.3 Urteil/""Ranking"" der Kontextarten hinsichtlich der Erhöhung der Netzwerksicherheit

3 Fähigkeiten

Zum gegenwärtigen Zeitpunkt fehlt mir noch ganz oder teilweise:

1. Wissen über die konkrete Funktionsweise/Übersicht über alle Funktionen der von mir gewählten IDS-Implementationen(zeek,suricata,evtl snort etc.)
2. Die Fähigkeit ein Netzwerk aufzusetzen
3. Kommasetzung
4. Das Wissen abschätzen zu können welcher Kontext wie enfach zu nutzen ist was eventuell zu Zeitproblemen/schlechtem Aufwand-Nutzen-Verhältnis bei der Implementierung führen könnte

4 Zeitplan

→ Excel-Template