Nidhogg

Betriebsdokumentation

Ives Schneider

Index

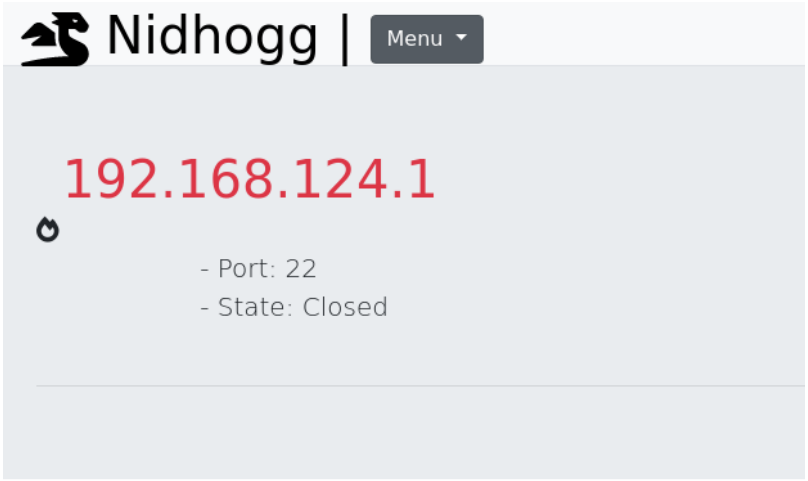
1. Login

Login kann direkt auf der Weboberfläche durchgeführt werden.
Username / Passwort entsprechen der Konfiguration unter `/etc/nidhogg/config.yml`.

Für das Sessionmanagement wird ein Session-Cookie gesetzt, welcher bei jedem request überprüft wird.

2. Scanresult

Sobald ein GET-Request zu /port gemacht wird, wird im Hintergrund ein Portscan auf die Geräte welcher unter `mappings.xml/portspecs.yml` definiert sind.
Falls eine Abweichung mit den definierten Spezifikationen gefunden werden sollte, wird hier die Information dargestellt.



3. Arpscan

Die aufgezeichneten ARP-Requests werden in der DB aufgezeichnet und können hier nachverfolgt werden.

Falls die Funktion deaktiviert sein sollte, wird hier eine Fehlermeldung angezeigt.

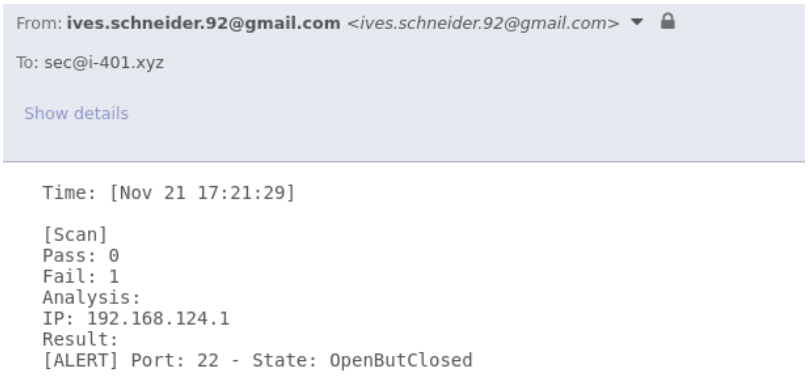
Da die Netzwerkkarte im Promiscous Modus laufen muss, könnten eventuelle Einschränkungen duch die Virtualisierungsengine auftreten.

4. Meldungen

Falls aktiviert werden in den definierten intervalen Mails and die angegebene Adresse gesendet.
Diese Mails werden nur gesendet, falls Anomalien gefunden werden.

4.1. Portscan

Für jede Anomalie sendet nidhogg ein eigenes Mail.



4.2. Arpscan

Der Arpscanner verhält sich gleich wie der Portscan und sendet direkt eine Mail, sobald ein neuer Host im Netz entdeckt werden würde.

5. Logout

Logout kann manuell durch den Aufruf von /logout gemacht werden.