Erik Brändli

Technologie ITSecX

Erik Brändli

Hüseyin Bozkurt

Nmap

Portscanner / Networkmapper

Contents

[Changelog 1](#_Toc422242147)

[Nmap.org 2](#_Toc422242148)

[Produktdaten 2](#_Toc422242149)

[Globale Anwendung 3](#_Toc422242150)

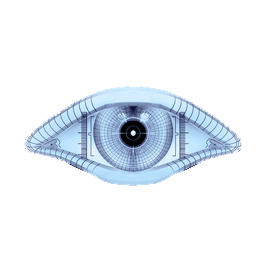
[Entscheidungsgrundlagen 3](#_Toc422242151)

# Changelog

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Datum* | *Name* | *Unterschrift* |
| Erstellt | 16.06.15 | Erik Brändli |  |
| Geprüft | 17.06.15 | Hüseyin Bozkurt |  |
| Freigegeben |  |  |  |

## Nmap.org

### Produktdaten

Erscheinungsjahr 1997  
Aktuelle Version 6.47  
programmiert in C, C++, Python, Lua

Nmap ist ein Werkzeug zum Scannen und Auswerten von Hosts in einem Computernetzwerk und fällt somit in die Kategorie der Portscanner. Der Name steht für Network Mapper.

Nmap wird in erster Linie für Portscanning (also das Untersuchen der Ports eines Hosts) eingesetzt. Das Werkzeug wurde ständig erweitert und konnte sich vor allem durch die aktiven Techniken für OS-Fingerprinting (das Erkennen des eingesetzten Betriebssystems auf dem Zielhost) einen Namen machen. Auch das Mapping von Umgebungen (Erkennen aktiver Hosts) ist möglich. Darüber hinaus lassen sich mit Nmap vereinzelt die hinter einem Port stehenden Dienste und deren Version auslesen.

Nmap ist sowohl bei Angreifern als auch bei Administratoren sehr beliebt, da es sehr effizient und zuverlässig arbeitet. Es ist ein wichtiger Bestandteil bei der Netzwerkdiagnose und Auswertung von netzwerkfähigen Systemen. Unter anderem wird es auch vom Vulnerability Scanner Nessus zur Erfassung offener Ports eingesetzt

## Globale Anwendung

Wird zur Entdeckung von Port und Diensten an einem System verwendet.  
Jedoch kann man bei diesem Portscanner auch die Version eines Dienstes überprüfen. Aus diesen Daten kann man evtl. Sicherheitslücken finden.

## Entscheidungsgrundlagen

Nmap unterstützt sowohl UDP (User Datagramm Protocol) als auch TCP (Transmission Control Protocol) und kann falls erfordert in den meisten Fällen auch die Version erkennen.

Nmap ist in der Lage das Betriebsystem des entfernten Hosts zu klassifizieren und analysieren.

Nmap läuft auf Windows als auch auf Linux stämmigen Betriebsystemen.

Die Scantypen sind modular und können nach Belieben weitere Funktionen beinhalten.

Nmap ist gratis und ohne Lizenz erhältlich.

Nmap wird laufend dokumentiert und verbessert, die Dokumentation beinhaltet Whitepapers aus auch Tutorien.