Erik Brändli

Technologie ITSecX

Erik Brändli

Hüseyin Bozkurt

SFTP

FileTransfer Technologie

Contents

[Changelog 1](#_Toc422242147)

[Nmap.org 2](#_Toc422242148)

[Produktdaten 2](#_Toc422242149)

[Globale Anwendung 3](#_Toc422242150)

[Entscheidungsgrundlagen 3](#_Toc422242151)

# Changelog

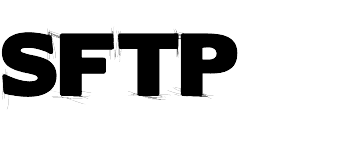
|  |  |  |  |
| --- | --- | --- | --- |
|  | *Datum* | *Name* | *Unterschrift* |
| Erstellt | 16.06.15 | Erik Brändli |  |
| Geprüft | 17.06.15 | Hüseyin Bozkurt |  |
| Freigegeben |  |  |  |

## SFTP

### Produktdaten

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

Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht.

Im Unterschied zum FTP über TLS (FTPS) begnügt sich SFTP mit einer einzigen Verbindung zwischen Client und Server. Diese Auslegung ermöglicht, dass SFTP freistellt, statt SSH jedwedes andere Verfahren zur Authentifizierung und Verschlüsselung einzusetzen.  
SFTP wurde von SSH Communications Security konzipiert. 2001 erfolgte die erste Veröffentlichung der Spezifikation durch die Internet Engineering Task Force. Die Vorbereitung des Entwurfs eines Internetstandards wurde 2006 aus organisatorischen Gründen abgebrochen.

Eingeführt wurde SFTP mit Version 2 der Secure Shell, deren Version 1 stattdessen Secure Copy bot

Viele Programme für Dateitransfer unterstützen SFTP und greifen zu diesem Zweck auf PuTTY oder OpenSSH zurück.

Diesen beiden Programmpaketen zu eigen sind Befehle wie get und put für Downloads und Uploads. SFTP definiert nur grundlegende Befehle für Programmierer, aber keine zusammengesetzten Befehle wie get und put für Benutzer

Wie auch SSH, wird SFTP üblicherweise auf Port 22 angeboten

## 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.