# TTP Detail – T1556.004

## TTP Information

Name: Network Device Authentication

Description: Adversaries may use [Patch System Image](https://attack.mitre.org/techniques/T1601/001) to hard code a password in the operating system, thus bypassing of native authentication mechanisms for local accounts on network devices.

[Modify System Image](https://attack.mitre.org/techniques/T1601) may include implanted code to the operating system for network devices to provide access for adversaries using a specific password. The modification includes a specific password which is implanted in the operating system image via the patch. Upon authentication attempts, the inserted code will first check to see if the user input is the password. If so, access is granted. Otherwise, the implanted code will pass the credentials on for verification of potentially valid credentials.(Citation: Mandiant - Synful Knock)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Malware

* SLOWPULSE
* SYNful Knock