# TTP Detail – T1078.001

## TTP Information

Name: Default Accounts

Description: Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS, the root user account in ESXi, and the default service account in Kubernetes.(Citation: Microsoft Local Accounts Feb 2019)(Citation: AWS Root User)(Citation: Threat Matrix for Kubernetes)

Default accounts are not limited to client machines; rather, they also include accounts that are preset for equipment such as network devices and computer applications, whether they are internal, open source, or commercial. Appliances that come preset with a username and password combination pose a serious threat to organizations that do not change it post installation, as they are easy targets for an adversary. Similarly, adversaries may also utilize publicly disclosed or stolen [Private Keys](https://attack.mitre.org/techniques/T1552/004) or credential materials to legitimately connect to remote environments via [Remote Services](https://attack.mitre.org/techniques/T1021).(Citation: Metasploit SSH Module)

Default accounts may be created on a system after initial setup by connecting or integrating it with another application. For example, when an ESXi server is connected to a vCenter server, a default privileged account called `vpxuser` is created on the ESXi server. If a threat actor is able to compromise this account’s credentials (for example, via [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212) on the vCenter host), they will then have access to the ESXi server.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)(Citation: Pentera vCenter Information Disclosure)

## Threat-Mapped Scoring

Score: 3.75

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: initial-access

## Malware

* HyperStack
* Stuxnet

## APTs (Intrusion Sets)

* Ember Bear
* FIN13
* Magic Hound