

Falco Training and Certification Course

Day - 1	
Securuing Containers (RASP)- Twistkock	Securuing Containers (RASP)- Falco
Falco Components	Spawned processes using execve
Userspace program	Falco drivers
Falco Configuration	Falco userspace program
Privilege escalation using privileged containers	• Executing shell binaries such as sh, bash, csh, zsh, etc
Namespace changes using tools like setns	• Executing SSH binaries such as ssh, scp, sftp, etc
• Read/Writes to well-known directories such as / etc, / usr/bin, / usr/sbin	Mutating Linux coreutils executables
Oreating symlinks	Mutating login binaries
Ownership and Mode changes	Mutating shadowutil or passwd executables
Unexpected network connections or socket mutations	