FortiDeceptor

Analysis Report

Total 1 record

Generated at 2019-09-24 03:33:07

Firmware Version: v2.1.0,build0142 (GA)

Filtering Criteria

ID	is	1190478637371270030

Summary of Incident

#	Severity		Start	End	Type	Attacker IP	Attacker User	Victim IP	Victim Port
23	■ ■ ■ ■	Critical	Sep 24 2019 03:16:16	Sep 24 2019 03:17:14	Interaction	10.1.108.2	manny	10.1.108.200	22

Incident Detail List

Interaction type incident on 10.1.108.200 (23)

Severity	Time	Event Type	Detail
Critical	Sep 24 2019 03:16:16	Execute command via SSH	ls
Critical	Sep 24 2019 03:16:16	Execute command via SSH	pwd
Critical	Sep 24 2019 03:16:16	Execute command via SSH	cd ..
Critical	Sep 24 2019 03:16:16	Execute command via SSH	ls
Critical	Sep 24 2019 03:16:16	Execute command via SSH	cd share/
Critical	Sep 24 2019 03:16:16	Execute command via SSH	ls
Critical	Sep 24 2019 03:16:16	Execute command via SSH	cd home/
Critical	Sep 24 2019 03:16:18	Execute command via SSH	ks
Critical	Sep 24 2019 03:16:20	Execute command via SSH	ls
Low Risk	Sep 24 2019 03:16:23	Open Port	22
High Risk	Sep 24 2019 03:16:23	Established SSH connection	10.1.108.2
High Risk	Sep 24 2019 03:16:23	Start SSH session	manny
Critical	Sep 24 2019 03:16:23	Execute command via SSH	User open child process on 1507
Critical	Sep 24 2019 03:16:23	Execute command via SSH	Starting session: shell on pts/1 for manny from 10.1.108.2 port 56518 id 0
Critical	Sep 24 2019 03:16:33	Execute command via SSH	clear
Critical	Sep 24 2019 03:16:36	Execute command via SSH	cd ..
Critical	Sep 24 2019 03:16:40	Execute command via SSH	clear
Critical	Sep 24 2019 03:16:42	Execute command via SSH	pwd
Critical	Sep 24 2019 03:16:45	Execute command via SSH	ls
Critical	Sep 24 2019 03:16:50	Execute command via SSH	cd home/
Critical	Sep 24 2019 03:16:51	Execute command via SSH	ls
Critical	Sep 24 2019 03:16:55	Execute command via SSH	cd share
Critical	Sep 24 2019 03:17:14	Execute command via SSH	ls