Team: Team 2

Inject Number: 29

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 01 Feb 2020 20:52:13 +0000

From: CISO

To: To Infrastructure Team

Subject: PDOM 3a - Implement/Configure SSH on Linux Servers

SSH is the only authorized remote access permissible on our Linux servers, Telnet and r-commands are insecure and against best practice. Since I am not 100% positive of the current status of our services, please respond with a business memo that includes the following components for each Linux system: 1) Document what daemons are running for remote access, specifically Telnet, r-commands, and//or SSH via a table; 2) Implement SSH on each Linux system for authorized users with no root logins permitted (Don't forget to enable sudo for authorized users to allow administration) and demonstrate through screenshots or other appropriate evidence in the memo for EACH system showing the proper configuration and operation; and 3) Disable other remote access daemons except SSH and demonstrate through screenshots or other appropriate evidence in the memo for EACH system that no other remote access daemons are enabled.

Thank you.

CISO