HKUST Ubuntu 14.04 LTS Hardening Guide V1.01

Last updated: 20160722

CIS Rule ID (v1.0.0)	Description
Patching and Software Updates	
1.1	Install Updates, Patches and Additional Security Software
OS Services	
5.1.1	Ensure NIS is not installed
5.1.2	Ensure rsh server is not enabled
5.1.3	Ensure rsh client is not installed
5.1.4	Ensure talk server is not enabled
5.1.5	Ensure talk client is not installed
5.1.6	Ensure telnet server is not enabled
5.1.7	Ensure tftp-server is not enabled
5.2	Ensure chargen is not enabled
5.3	Ensure daytime is not enabled
5.4	Ensure echo is not enabled
5.5	Ensure discard is not enabled
5.6	Ensure time is not enabled
6.1	Ensure the X Window system is not installed
6.5	Configure Network Time Protocol (NTP)
6.9	Ensure FTP Server is not enabled
Network Configuration and Firewalls	
7.7	Ensure Firewall is active
Logging and Auditing	
8.1.2	Install and Enable auditd Service
8.1.3	Enable Auditing for Processes That Start Prior to auditd
8.1.8	Collect Login and Logout Events
8.1.14	Collect File Deletion Events by User
System Access, Authentication and Authorization	
9.2.1	Set Password Creation Requirement Parameters Using pam_cracklib
9.2.2	Set Lockout for Failed Password Attempts. Set lockout for 5 failed password attempts
9.2.3	Limit Password Reuse. Prohibit reuse past 5 passwords
9.3.8	Disable SSH Root Login
9.4	Restrict root Login to System Console
User Accounts and Environment	
10.1.1	Set Password Expiration Days to 90 days
10.1.3	Set Password Expiring Warning Days to 7 days advance
Review User and Group Settings	
13.1	Ensure Password Fields are Not Empty
13.5	Verify No UID 0 Accounts Exist Other Than root
Reference	**https://benchmarks.cisecurity.org/tools2/linux/CIS_Ubuntu_14.04_LTS_Server_Benchmark_v1.0.0.pdf**