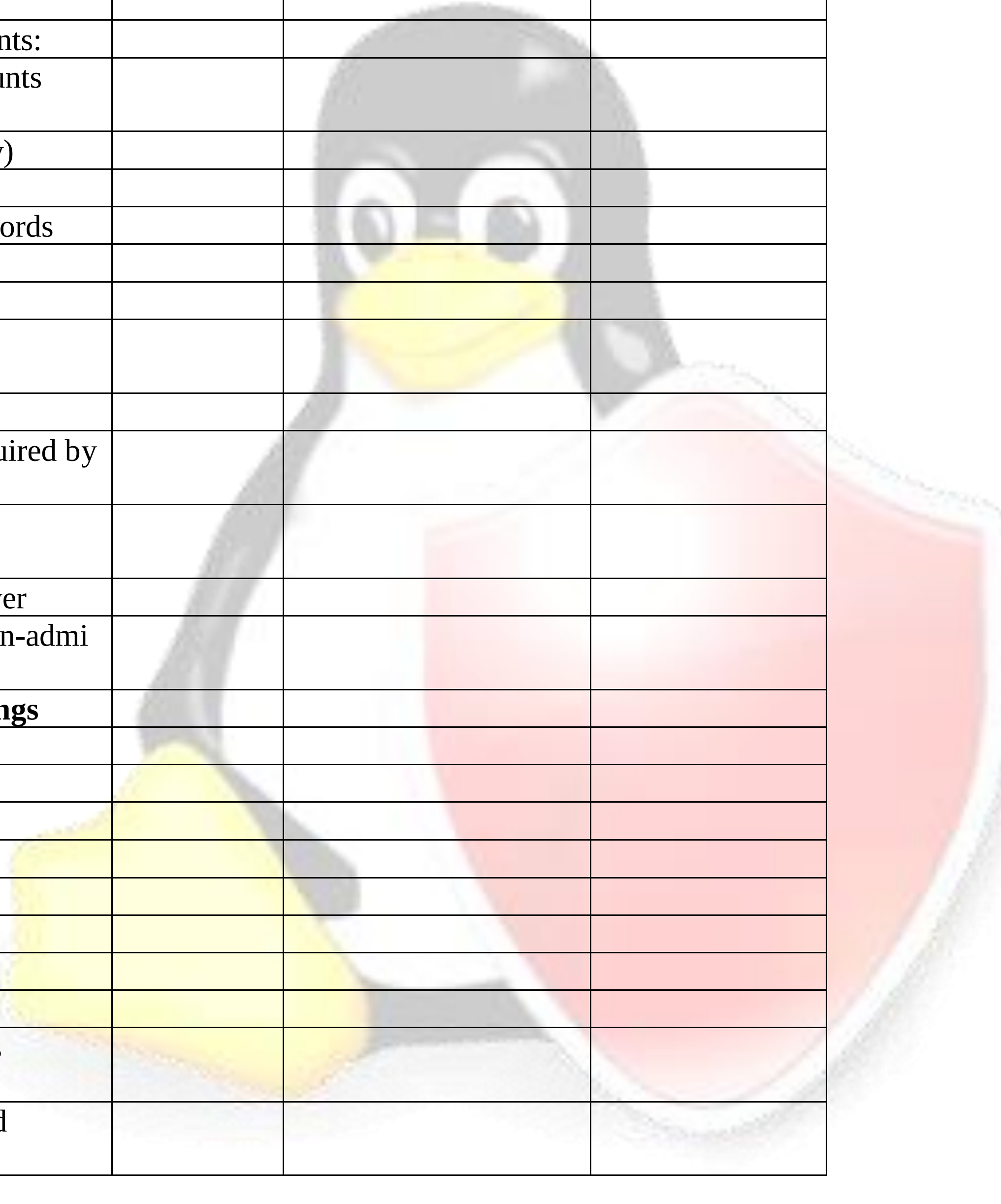
NUST CYBER SECURITY TEAM

Linux security hardening Checklist

Task	Time	Person/s Responsible	Task Completed
Change default passwords			
Change all user passwords			
Change all service passwords			
Verify No Accounts Have Empty Passwords			
Lock all empty password accounts:			
Make Sure No Non-Root Accounts Have UID Set To 0			
Disable root Login (if necessary)			
Password Policy			
Enforce the use of strong passwords			
Apply Security Patches			
Update system			
Identifying and disabling unnecessary services			
Disable unnecessary services			
Disable ports which are not required by the system.			
Prevent information revealed through system scanning			
Secure Apache/PHP/Nginx server			
Run apache with a dedicated non-admi n account			
Remote Access and SSH Settings			
PermitRootLogin no			
PermitEmptyPasswords no			
Banner /etc/issue			
IgnoreRhosts yes			
RhostsAuthentication no			
RhostsRSAAuthentication no			
HostbasedAuthentication no			
LoginGraceTime 1m			
SyslogFacility AUTH (provides logging under syslog AUTH)			
AllowUser [list of users allowed access]			



DenyUser [list of system accounts not allowed]			
System Logging and Auditing			
/var/log/message: General message and system related stuff			
/var/log/auth.log: Authenication logs			
/var/log/cron.log: Crond logs (cron job)			
/var/log/maillog: Mail server logs			
/var/log/httpd/: Apache access and error logs directory			
/var/log/secure: Authentication log			
/var/log/mysqld.log: MySQL database server log file			
Install an integrity Checking Software			
Install an IDS & IPS tool eg fail2ban			
Configure firewall/IP Tables			
Backups			
Database backup			
Website backup			