	group_code	group_name	title_code	title_name	important	decision	
0	G01	1.	G0101	1.01 root			\n□ \n , root \n\n■ \n\n \n① Telnet \n--\n▷ Telnet Service disable\n \n \n① SSH \n--\nro? 00:00:00 sshd: tw0n3 [priv]\ntw0n3 141860 141729 0 17:39 ? 00:00:00 sshd: tw0n3@pts/2\n \n▷ SSH Service Enable\n \n \n② sshd_config \n----------------------------------
1	G01	1.	G0102	1.02			\n□ \n·· 2 10 , 3 8 (9)\n\n■ \n\n① /etc/shadow _\nroot:6BfC3zlKE93CBn4/P$.3LAje6XtzpsPV5P9sCHBWorDgej7p6PfkaLwVAESNx569zFH2dRh.oLcudAuYvSt6JdpAzTdCoey21wWdCzh.:19\n/etc/pam.d/system-auth: No such file or directory\n \n---\n \n③ Linux 7.x /etc/security/pwquality.conf \n/etc/security/pwquality.conf .\n \n--\n[1.02] TIP\n \nmd5 = $ 1 $ \nsha256 = $ 5 $ \nsha512 = $ 6 $ \n \n \n
2	G01	1.	G0103	1.03			\n□ \n 10 \n\n■ \n\n/etc/pam.d/system-auth .\n \n[1.03] \n \n \n
3	G01	1.	G0104	1.04			\n□ \n , \n\n■ \n\n[/etc/passwd]\nroot:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\nga data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/irc Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin\nsystemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin\nmessagebus:x:103:106::/nonexistent:/usr/sbin/nologin\nsys stack,,,:/var/lib/tpm:/bin/false\nuuidd:x:107:112::/run/uuidd:/usr/sbin/nologin\ntcpdump:x:108:113::/nonexistent:/usr/sbin/nologin\nlandscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin\npollina \n[/etc/shadow]\nroot:6BfC3zlKE93CBn4/P$.3LAje6XtzpsPV5P9sCHBWorDgej7p6PfkaLwVAESNx569zFH2dRh.oLcudAuYvSt6JdpAzTdCoey21wWdCzh.:19063:0:99999:7:::\ntw0n3:6qzseUfe.v
4	G01	1.	G0105	1.05 root uid '0'			\n□ \nroot UID \n\n■ \n\nroot -> UID=0\n \n[/etc/passwd]\nroot:x:0:0:root:/root:/bin/bash\n \n[1.05] \n \n \n
5	G01	1.	G0106	1.06 root su			\n□ \nsu \npam su (4750) \n\n■ \n\n① /etc/pam.d/su pam_wheel.so \n---\n▷ pam \n \n \n② su (/usr/bin/su) \n----------------------------------\n\nroot:x:0:\ndaemon:x:1:\nbin:x:2:\nsys:x:3:\nadm:x:4:syslog,tw0n3\ntty:x:5:syslog\ndisk:x:6:\nlp:x:7:\nmail:x:8:\nnews:x:9:\nuucp:x:10:\nman:x:12:\nproxy:x:13:\nkmem:x:15:\ndialout:x:20:\nfax:x:2 data:x:33:\nbackup:x:34:\noperator:x:37:\nlist:x:38:\nirc:x:39:\nsrc:x:40:\ngnats:x:41:\nshadow:x:42:\nutmp:x:43:\nvideo:x:44:\nsasl:x:45:\nplugdev:x:46:tw0n3\nstaff:x:50:\ngames:x:60:\nusers:x:10 coredump:x:999:\ntw0n3:x:1000:\ndocker:x:998:\n \n[1.06] \n \n \n
6	G01	1.	G0107	1.07			\n□ \n 8 (9)\n\n■ \n\n[ ]\n#PASS_MIN_LEN\n \n[1.07] \n \n \n
7	G01	1.	G0108	1.08			\n□ \n 90(12) \n\n■ \n\n[ ]\nPASS_MAX_DAYS\t99999\n\n \n[1.08] \n \n \n
8	G01	1.	G0109	1.09			\n□ \n 1(1) \n\n■ \n\n[ ]\nPASS_MIN_DAYS\t0\n \n[1.09] \n \n \n
9	G01	1.	G0110	1.10			\n□ \n \n \n\n■ \n\n① (adm, lp, sync, shutdown, halt, news, uucp, nuucp, operator, games, gopher, nfsnobody, squid) \n--\ngames:x:5: in**\nbin **Never logged in**\nsys **Never logged in**\nsync **Never logged in**\ngames **Never logged in**\nman **Never logged in**\nlp **Never logged in**\nmail **Never logged in**\nnews * timesync **Never logged in**\nmessagebus **Never logged in**\nsyslog **Never logged in**\n_apt **Never logged in**\ntss **Never logged in**\nuuidd **Never logged in**\ntcpdump **Never logg
10	G01	1.	G0111	1.11			\n□ \n ( )\n\n■ \n\n[ ]\nroot:x:0:\n \n[1.11] \n \n \n
11	G01	1.	G0112	1.12 GID			\n□ \n GID ( )\n\n■ \n\n▷ \n---\nadm 4\ntty 5\ndisk 6\nkmem 15\ndialout 20\nfax 21\nvoice 22\ncdrom 24\nfloppy 25\ntape 26\nsudo 27\na
12	G01	1.	G0113	1.13 UID			\n□ \n UID \n UID .\n \n[1.13] \n \n \n
13	G01	1.	G0114	1.14 Shell			\n□ \n /bin/false(nologin) \n\n■ \n\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\ngames:x:5:60:games:/usr/games: Synchronization,,,:/run/systemd:/usr/sbin/nologin\nsyslog:x:104:110::/home/syslog:/usr/sbin/nologin\nsystemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin\n \n /bin/false(nologi
14	G01	1.	G0115	1.15 Session Timeout			\n□ \nSession Timeout 600(10) \n\n■ \n\n① /etc/profile \n--\n/etc/profile TMOUT/TIMEOUT .\n \n/etc/csh.login, /etc/csh.cshrc .\n \n[1.15] \n \n
15	G02	2.	G0201	2.01 root ,			\n□ \nPATH '.' \n\n■ \n\n \n① PATH \n--\n/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin\n \n[2.01] \n \n \n
16	G02	2.	G0202	2.02			\n□ \n \n\n■ \n\n① (=> :)\n--\n .\n \n[2.02] \n \n \n
17	G02	2.	G0203	2.03 /etc/passwd			\n□ \n/etc/passwd root, 644 \n\n■ \n\n① /etc/passwd \n--\n-rw-r--r-- 1 root root 1824 Feb 27 08:24 /etc/passwd\n \n[2.03] \n \n \n
18	G02	2.	G0204	2.04 /etc/shadow			\n□ \n/etc/shadow root, 400 \n\n■ \n\n① /etc/shadow \n---\n-rw-r----- 1 root shadow 1157 Mar 12 14:33 /etc/shadow\n \n[2.04] \n \n \n
19	G02	2.	G0205	2.05 /etc/hosts			\n□ \n/etc/hosts root, 600 \n\n■ \n\n① /etc/hosts \n--\n-rw-r--r-- 1 root adm 233 Feb 26 23:37 /etc/hosts\n \n[2.05] \n \n \n
20	G02	2.	G0206	2.06 /etc/(x)inetd.conf			\n□ \n/etc/(X)inetd.conf root, 600 \n\n■ \n\n/etc/xinetd.d .\n \n/etc/xinetd.conf .\n \n/etc/inetd.conf .\n \n \n[2.06] \n \n \n
21	G02	2.	G0207	2.07 /etc/syslog.conf			\n□ \n/etc/syslog.conf root, 644 \n\n■ \n\n▷ rsyslog.conf \n-rw-r--r-- 1 root root 1382 Feb 12 2020 /etc/rsyslog.conf\n /etc/syslog-ng.conf \n \n[2.07] \n \n \n
22	G02	2.	G0208	2.08 /etc/services			\n□ \n/etc/service root, 644 \n\n■ \n\n① /etc/services \n--\n-rw-r--r-- 1 root root 14464 Feb 17 2020 /etc/services\n \n[2.08] \n \n \n
23	G02	2.	G0209	2.09 SUID, SGID, Sticky bit			\n□ \n SUID SGID \n\n■ \n\n/sbin/dump \n/usr/bin/lpq-lpd \n-rwsr-xr-x 1 root root 44784 Jul 15 2021 /usr/bin/newgrp\n/sbin/restore \n/usr/bin/lpr \n/usr/sbin/lpc \n-rwxr-sr-x 1 root shadow 4
24	G02	2.	G0210	2.10 ,			\n□ \n root , root \n■ \n-rw-r--r-- 1 tw0n3 tw0n3 894 Feb 27 01:41 /home/tw0n3/.profile\n-rw-r--r-- 1 tw0n3 tw0n3 3771 Mar 9 16:37 /home/tw0n3/.bashrc\n-rw------- 1 tw0n3 tw0n3 20085
25	G02	2.	G0211	2.11 world writable writable			\n□ \nworld writable , \n\n■ \nWorld Writable \n--\ndrwxrwxrwt : root : root : /var/crash\ndrwxrwxrwt : roo upower.service-4ru5Qg/tmp\ndrwxrwxrwt : root : root : /var/tmp/systemd-private-e1f85286dca840969c9a8c79988fb0d7-fwupd.service-IDbRng/tmp\ndrwxrwxrwt : root : root : /var/tmp/systemd-priv /tmp/systemd-private-e1f85286dca840969c9a8c79988fb0d7-fwupd.service-wpxi5h/tmp\ndrwxrwxrwt : root : root : /tmp/.XIM-unix\ndrwxrwxrwt : root : root : /tmp/systemd-private-e1f85286dca840 IxbS7h/tmp\ndrwxrwxrwt : root : root : /tmp/snap.lxd/tmp\ndrwxrwxrwt : root : root : /tmp/.Test-unix\n-rwxrwxrwx : tw0n3 : tw0n3 : /home/tw0n3/CAT-CERT/Out-Sourcing/ESS/OS_Linux_v2.1.sh\n-r tw0n3 : /home/tw0n3/pwn/study/test/DROP\n 25 \n[2.11] \n\n
26	G02	2.	G0212	2.12 /dev device			\n□ \ndev device \n■ \n① : find /dev -type f -exec ls -l {} \;\n--\n▷ /dev Device .\n \n (charactor, block file) : find /dev -type [C B] -exe 15:15 /dev/sr0\nbrw-rw---- 1 root disk 8, 3 Mar 12 15:15 /dev/sda3\nbrw-rw---- 1 root disk 8, 2 Mar 12 15:15 /dev/sda2\nbrw-rw---- 1 root disk 8, 1 Mar 12 15:15 /dev/sda1\nbrw-rw---- 1 root disk 8, 0 rw---- 1 root disk 7, 2 Mar 12 15:15 /dev/loop2\nbrw-rw---- 1 root disk 7, 1 Mar 12 15:15 /dev/loop1\nbrw-rw---- 1 root disk 7, 0 Mar 12 15:15 /dev/loop0\n \n[2.12] \n---------------------------------
27	G02	2.	G0213	2.13 $HOME/.rhosts, hosts.equiv			\n□ \nexec(512/tcp), login(513/tcp), shell(514/tcp) , \n1. /etc/hosts.equiv /root/.rhosts root , \n2. /etc/hosts.equiv /root/.rhosts 600 \n3. /etc/hosts.equiv /root/.rhosts '+' \n■ \n\n■ \n--
28	G02	2.	G0214	2.14 IP			\n□ \n/etc/hosts.deny ALL Deny , /etc/hosts.allow \n■ \n/etc/hosts.deny \n# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.\n# See the manual pages hosts_access(5) host whose name does not match its\n# address.\n#\n# You may wish to enable this to ensure any programs that don't\n# validate looked up hostnames still leave understandable logs. In past\n# you're going to protect the portmapper use the name "rpcbind" for the\n# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.\n#\n\n \n[2.14] \n\n
29	G02	2.	G0215	2.15 hosts.lpd			\n□ \nhosts.lpd root, 600 \n■ \n/etc/hosts.lpd \n \n[2.15] \n\n
30	G02	2.	G0216	2.16 UMASK			\n□ \nUMASK 022 \n■ \n▷ UMASK (root umask) \n0022\n \n▷ /etc/profile \n \n▷ /etc/bashrc \n/etc/bashrc .()\n \n[2.16] \n\n
31	G02	2.	G0217	2.17			\n□ \n , \n■ \ndrwxr-xr-x 19 root root 4096 Feb 26 23:22 /\ndrwxr-xr-x 21 root root 4340 Mar 15 14:37 /dev\ndrwxr-xr-x 19 tw0n3 tw0n3 4096 Mar 24 14:36 /home/tw0n3\ndrwx------ 7 root ro
32	G02	2.	G0218	2.18			\n□ \n \nroot '/' \n■ \n \n---\n \n \nroot '/' \n--\nroot '/' .\n \n[2.18] \n\n

33	G02	2.	G0219	2.19			\n□ \n , \n■ \n \n--\n \n \n[2.19] \n\n
34	G03	3.	G0301	3.01 finger			\n□ \nFinger \n■ \nfinger \n-------------------------------------\nfinger \n \n finger Service Disable\n \n[3.01] \n\n
35	G03	3.	G0302	3.02 Anonymous FTP			\n□ \nAnonymous FTP (ftp) \n : FTP, ProFTP ftp , vsFTP anonymous_enable \n■ \nFTP \n--\n \ntw0n3 83898 83897 0 Mar23 ? 00:00:00 /usr/
36	G03	3.	G0303	3.03 r			\n□ \nr \n■ \n \n------------------------ \nr command Sevice Disable\n \n[3.03] \n \n\n
37	G03	3.	G0304	3.04 cron			\n□ \ncron root, 640 \n OS \n■ \nCron \n----------------------------\nroot 894 1 0 Mar21 ? 00:00:01 /usr/sbin/cron -f\n \n▷ cron Service Enable\n \nCron \n----------------------------\n-rwxr-sr-x 1 /etc/cron.daily/dpkg\n-rwxr-xr-x 1 root root 17357 Feb 27 03:09 /etc/cron.daily/google-chrome\n-rwxr-xr-x 1 root root 377 Jan 21 2019 /etc/cron.daily/logrotate\n-rwxr-xr-x 1 root root 1123 Feb 26 2 /etc/cron.weekly/update-notifier-common\n\n/var/spool/cron/atjobs \n\n/var/spool/cron/atspool \n\n/var/spool/cron/crontabs \n \nCron.allow, Cron.deny \n----------------------------\n/etc/cron.deny \n/etc/cron.a
38	G03	3.	G0305	3.05 Dos			\n□ \nDoS echo, discard, daytime, chargen \n■ \ninetd.conf echo, discard, daytime, chargen \n-- \n/etc/inetd.conf \n \n \n/etc/xinetd.d \n------------------------\n\
39	G03	3.	G0306	3.06 NFS			\n□ \nNFS \n■ \nNFS Server Daemon(nfsd)\n---\nNFS Service Disable\n \nNFS Client Daemon(statd,lockd)\n----------------------
40	G03	3.	G0307	3.07 NFS			\n□ \nNFS , everyone \n■ \n \nNFS Service Disable\n \n[3.07] \n\n
41	G03	3.	G0308	3.08 automountd			\n□ \nautomountd \n■ \nAutomount \n \nautomount .\n \n[3.08] \n\n
42	G03	3.	G0309	3.09 RPC			\n□ \n RPC \n■ \ninetd.conf RPC \n------------------------------------ \n/etc/inetd.conf \n \n \n/etc/xinetd.d \n------------------------\n/etc/xinetd.d . \n \n \n/etc/xinetd.d \n---------------------\n \n[3.09] \n\
43	G03	3.	G0310	3.10 NIS, NIS+			\n□ \nNIS , NIS+ \n■ \nNIS, NIS+ Service Disable\n \n[3.10] \n\n
44	G03	3.	G0311	3.11 tftp, talk			\n□ \ntftp, talk, ntalk \n■ \ninetd.conf tftp, talk \n------------------------------------ \n/etc/inetd.conf \n \n \n/etc/xinetd.d \n------------------------\n \n/etc/xinetd.d \n----------------------\n \ntftp, talk, ntalk \n---
45	G03	3.	G0312	3.12 Sendmail			\n□ \nSendmail (21.06.04 8.16.1)\n■ \nSendmail \n----------------------------------- \n \n▷ Sendmail Service Disable\n \n/etc/mail/sendmail.cf, /etc/sendmail.cf \n \n[3.12] \n\n
46	G03	3.	G0313	3.13			\n□ \nSMTP \n■ \nSendmail \n------------------------------------- \nSendmail Service Disable\n \n \n/etc/mail/sendmail.cf \n------------------------------------ \n/etc/mail/sendmail.cf \n \n[3.13] \n\n
47	G03	3.	G0314	3.14 sendmail			\n□ \nSMTP , Sendmail (restrictqrun)\n■ \nSendmail \n------------------------------------ \n \n▷ Sendmail Service Disable\n \n/etc/mail/sendmail.cf \n------------------------------------ \n/etc/mail/sendmail.cf
48	G03	3.	G0315	3.15 DNS			\n \n▷ DNS Service Disable\n \n
49	G03	3.	G0316	3.16 DNS Zone Transfer			\n \n① DNS \n----------------------------------- \n▷ DNS Service Disable\n \n② /etc/named.conf allow-transfer \n------------------------------------ \n/etc/named.conf \n \n③ /etc/named.boot xfrnets \n------------
50	G03	3.	G0317	3.17			\n▷ \n
51	G03	3.	G0318	3.18			\n▷ \n \n
52	G03	3.	G0319	3.19			\n▷ \n \n
53	G03	3.	G0320	3.20			\n▷ \n \n
54	G03	3.	G0321	3.21			\n▷ \n \n
55	G03	3.	G0322	3.22			\n▷ \n \n
56	G03	3.	G0323	3.23			\n▷ \n \n
57	G03	3.	G0324	3.24 ssh			\n① \n---\nroot 4170 1 0 Mar21 ? 00:00:00 sshd: tw0n3 [priv]\ntw0n3 4254 4170 0 Mar21 ? 00:00:08 sshd: tw0n3@pts/1\nroot 83763 1 0 Mar23 ? \n---\nSSH (/etc/ssh/sshd_config): X (Default : 22)\n \n③ \n--\ntcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN \ntcp6 0 0 :::22 :::* LISTEN \
58	G03	3.	G0325	3.25 ftp			\n□ /etc/services \n--\n(1)/etc/service:ftp 21/tcp\n(2)VsFTP : VsFTP .\n(3)ProFTP : ProFTP .\n \n② \n-------
59	G03	3.	G0326	3.26 ftp shell			\n▷ FTP Service Enable\n \n① ftp (ftp false nologin)\n--\nftp .\n
60	G03	3.	G0327	3.27 ftpuser			\n▷ FTP Service Enable\n \n /etc/ftpd/ftpusers .\n \n /etc/ftpusers .\n \n /etc/vsftpd.ftpusers .\n \n /etc/vsftpd/ftpusers .\n \n /etc/vsftpd.user_list .\n \n /etc/vsftpd/user_list .\n
61	G03	3.	G0328	3.28 ftpuser			\n▷ ftp Service Disable\n
62	G03	3.	G0329	3.29 at			\n/etc/at.allow .\n/etc/at.deny .\n-rw-r----- 1 root daemon 144 Nov 13 2018 /etc/at.deny\n \n■/etc/at.deny \n---------------------\nalias\nbackup\nbin\ndaemon\nftp\ngames\ngnats\nguest\nirc\nlp\nmail\
63	G03	3.	G0330	3.30 SNMP			\n① SNMP \n \n▷ SNMP Service Disable. \n
64	G03	3.	G0331	3.31 SNMP Community String			\n① SNMP \n \nSNMP . \n \n \n② Default CcmunityString \n---\n■ /etc/snmpd.conf .\n \n■ /etc/snmpdv3.conf .\n \n■ /etc/snmp/snmpd.conf .\n \
65	G03	3.	G0332	3.32			\n① (/etc/motd) \n--\n/etc/motd .\n \n② SSH \n--\n▷ SSH Service Enable\n \n■ ssh \nSSH
66	G03	3.	G0333	3.33 NFS			\n▷ NFS Service Disable\n
67	G03	3.	G0334	3.34 expn, vrfy			\n▶ : SMTP , noexpn, novrfy \n▶ \n \n① Sendmail \nSendmail Service Disable\n \n② /etc/mail/sendmail.cf \n/etc/mail/sendmail.cf \n
68	G03	3.	G0335	3.35 Apache			\n▶ : ServerTokens Prod \n▶ \n \n▷ \n \n
69	G04	4.	G0401	4.01			\n▶ : ( )\n▶ \n \n
70	G05	5.	G0501	5.01			\n▶ : , , \n▶ \n \n▷ \n \n
71	G05	5.	G0502	5.02			\n▶ : \n \n \n▷ syslog \nmessage+ 895 1 0 Mar21 ? 00:00:06 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only\nsyslog 905 1 0 Mar21 ? 0640\n$DirCreateMode 0755\n$Umask 0022\n$PrivDropToUser syslog\n$PrivDropToGroup syslog\n$WorkDirectory /var/spool/rsyslog\n$IncludeConfig /etc/rsyslog.d/*.conf\n \n■ /etc/syslog-ng.con