Linux伺服器安全基準

系統帳號管理-administrator帳號設定
UID=0之帳號

ID	TWGCB-01-003-0068
說明	• 檢測除了root帳號外，其他帳號之UID是否允許設為0(UID=0之帳號具有系統管理權限)
檢測方法	awk -F: '($3=="0"){print}' /etc/passwd
GCB設定值	應只有root開頭之行

```
[house@Centos ~]$ awk -F: '($3=="0"){print}' /etc/passwd
root:x:0:0:root:/root:/bin/bash
[house@Centos ~]$ awk -F: '($1!="root" && $3=="0"){print}' /etc/passwd
[house@Centos ~]$
```

Linux伺服器安全基準

系統功能關閉設定
非root系統帳號登入方式

ID	TWGCB-01-003-0065
說明	• 非root系統帳號是除root外，UID小於500之帳號，與一般使用者無關，是為了執行相關管理功能而存在於系統中。 • 針對非root系統帳號進行密碼鎖定與設定無法登入的合法shell(/sbin/nologin)，以提高攻擊者使用這些帳號進行攻擊之難度。
檢測方法	awk -F: '($3<500){print $1 ":" $3 ":" $7}' /etc/passwd
GCB設定值	/sbin/nologin

```
root:0:/bin/bash
bin:1:/sbin/nologin
daemon:2:/sbin/nologin
adm:3:/sbin/nologin
lp:4:/sbin/nologin
sync:5:/bin/sync
shutdown:6:/sbin/shutdown
halt:7:/sbin/halt
```

安全性事件設定-var/log單一記錄檔大小設定

日誌檔輪替服務

ID	TWGCB-01-003-0144
說明	• 決定是否啟用日誌檔輪替(logrotate)服務。
檢測方法	• 執行下列指令：$cat /etc/logrotate.d/syslog 確認含有以下字串： /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/cron
GCB設定值	啟用

Linux伺服器安全基準

日誌檔檢視服務

ID	TWGCB-01-003-0145
說明	• 決定是否啟用日誌檔檢視(logwatch)服務
檢測方法	執行下列指令： #ls –la /etc/cron.daily/0logwatch 確認內容顯示如下： 0logwatch->/usr/share/logwatch/scripts/logwatch.pl
GCB設定值	啟用

```
[root@tpetrainning-1 cron.daily]# ln -sf /usr/share/logwatch/scripts/logwatch.pl 0logwatch
[root@tpetrainning-1 cron.daily]# ls -la 0logwatch
lrwxrwxrwx. 1 root root 39 Sep  8 12:32 0logwatch -> /usr/share/logwatch/scripts/logwatch.pl
[root@tpetrainning-1 cron.daily]#
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則
使用空白密碼之帳號登入方式

ID	TWGCB-01-003-0066
說明	• 使用空白密碼意謂著任何人皆可以此帳號登入系統，並以該帳號之權限執行相關指令，將可能危害系統安全
檢測方法	awk -F: '($2==""){print}' /etc/passwd
GCB設定值	應為空白，若非，則設定該帳號密碼

```
[house@Centos ~]$ awk -F: '($2==""){print}' /etc/passwd
[house@Centos ~]$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

所有帳號的密碼遮蔽

ID	TWGCB-01-003-0067
說明	• 基於驗證程序需要，成功登入系統的使用者可讀取/etc/passwd檔案內容。如要避免密碼外洩，可利用遮蔽密碼方法，將密碼抽離出來，放在另一個只有root可以讀取的檔案中
檢測方法	awk -F: '($2!="x"){print}' /etc/passwd
GCB設定值	應為空值

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼最短使用期限

ID	TWGCB-01-003-0069
說明	• 檢測在使用者變更密碼之前，密碼必須使用的期限(天數)。設為0代表可隨時變更密碼，設為-1代表停用此原則 • 設定密碼最短使用期限為1天，以避免使用者重複使用相同密碼
檢測方法	grep ^PASS_MIN_DAYS /etc/login.defs
GCB設定值	PASS_MIN_DAYS 1

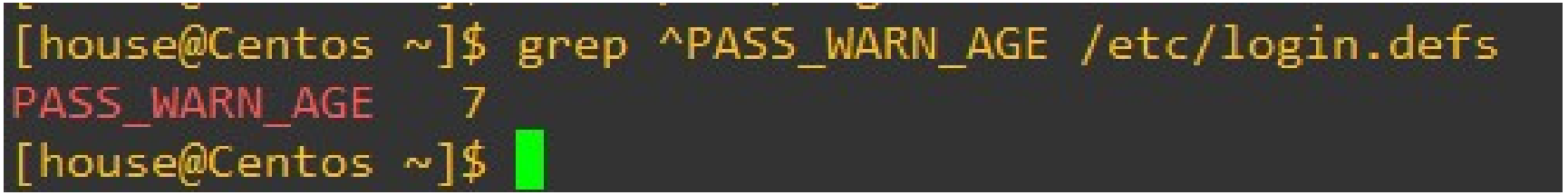
```
[house@Centos ~]$ grep ^PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS   0
[house@Centos ~]$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼到期前提醒使用者變更密碼

ID	TWGCB-01-003-0070
說明	• 檢測使用者密碼即將到期時，要提前多久(天數)提醒使用者進行密碼變更，設為-1代表停用此原則
檢測方法	grep ^PASS_WARN_AGE /etc/login.defs
GCB設定值	PASS_WARN_AGE 14



Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼最長使用期限

ID	TWGCB-01-003-0071
說明	• 檢測系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。設為-1代表停用此原則 • 根據環境而定，安全性的最佳作法是讓密碼每30至90天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限。
檢測方法	grep ^PASS_MAX_DAYS /etc/login.defs
GCB設定值	PASS_MAX_DAYS 60

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼最小長度

ID	TWGCB-01-003-0072
說明	• 檢測使用者帳號的密碼可包含的最少字元數。 • 若使用PAM模組管理密碼，pam_cracklib.so將會檢驗密碼相關的資訊，並且取代/etc/login.defs內的PASS_MIN_LEN 的設定。
檢測方法	grep ^PASS_MIN_LEN /etc/login.defs
GCB設定值	PASS_MIN_LEN 12

```
[house@Centos ~]$ grep ^PASS_MIN_LEN /etc/login.defs
PASS_MIN_LEN    5
[house@Centos ~]$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

可設定密碼次數

ID	TWGCB-01-003-0076
說明	• 決定重新設定密碼時，若密碼強度不符系統要求，在設定密碼狀態，可以連續輸入密碼之次數
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取retry
GCB設定值	retry=3

```
b10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
assword    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=
b10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼必須至少包含數字個數

ID	TWGCB-01-003-0077
說明	• 決定使用者帳號的密碼至少包含幾個數字
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取dcredit
GCB設定值	dcredit=1

```
mb10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-
1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼必須至少包含大寫字母個數

ID	TWGCB-01-003-0078
說明	• 決定使用者帳號的密碼至少包含幾個大寫字母
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取ucredit
GCB設定值	ucredit=1

```
mb10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-
1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼必須至少包含小寫字母個數

ID	TWGCB-01-003-0079
說明	• 決定使用者帳號的密碼至少包含幾個小寫字母
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取lcredit
GCB設定值	lcredit=1

```
mb10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-
1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼必須至少包含特殊字元個數

ID	TWGCB-01-003-0080
說明	• 決定使用者帳號的密碼至少包含幾個特殊字元
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取ocredit
GCB設定值	ocredit=1

```
mb10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-
1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

新密碼與舊密碼最少相異字元數

ID	TWGCB-01-003-0081
說明	• 決定使用者帳號的新密碼內必須有幾個字元與舊的密碼不同
檢測方法	• grep pam_cracklib.so /etc/pam.d/system-auth • 讀取difok
GCB設定值	difok=3

```
mb10@tpetrainning-1:~$ grep pam_cracklib.so /etc/pam.d/system-auth
password    requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-
1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

強制執行密碼歷程記錄

ID	TWGCB-01-003-0084
說明	• 決定重複使用舊密碼前，必須與使用者帳號相關的唯一新密碼數目
檢測方法	grep "remember" /etc/pam.d/system-auth
GCB設定值	remember=24

```
mb10@tpetrainning-1:~$ grep "remember" /etc/pam.d/system-auth
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_a
thtok existing_options remember=24
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-密碼原則

密碼雜湊演算法

ID	TWGCB-01-003-0083
說明	• 決定系統所採用之密碼雜湊演算法
檢測方法	• authconfig --test | grep hashing | grep sha512
GCB設定值	sha512

```
mb10@tpetrainning-1:~$ authconfig --test | grep hashing | grep sha512
 password hashing algorithm is sha512
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

安全性相關稽核事件設定-本機安全性原則-帳戶原則-帳戶鎖定原則

帳戶鎖定閾值

ID	TWGCB-01-003-0082
說明	• 決定使用者帳號被鎖定的嘗試登入失敗次數，以降低密碼暴力攻擊之影響
檢測方法	• grep pam_tally2.so /etc/pam.d/system-auth • 讀取deny
GCB設定值	deny=5

```
mb10@tpetrainning-1:~$ grep pam_tally2.so /etc/pam.d/system-auth
auth        required pam_tally2.so deny=5 onerr=fail
mb10@tpetrainning-1:~$
```

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

auditd服務

ID	TWGCB-01-003-0146
說明	• 決定是否啟用auditd服務
檢測方法	執行下列指令，確認所有執行層級皆設為啟用： #systemctl list-unit-files|grep auditd
GCB設定值	啟用

```
root@tpetrainning-1:~# systemctl list-unit-files|grep auditd
auditd.service                                enabled
```

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄變更日期與時間事件

ID	TWGCB-01-003-0148
說明	• 決定是否記錄變更日期或時間資訊之事件
檢測方法	執行下列指令： #sudo grep time_change /etc/audit/audit.rules ・確認包含下列內容： -a always,exit -F arch=(b32或b64) -S adjtimex -S settimeofday -S stime -k time-change -a always,exit -F arch=(b32或b64) -S clock_settime –k time-change -w /etc/localtime -p wa -k time-change
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄變更使用者或群組資訊事件

ID	TWGCB-01-003-0149
說明	• 決定是否記錄變更使用者或群組資訊之事件
檢測方法	執行下列指令： #sudo grep identity /etc/audit/audit.rules 確認包含下列內容： -w /etc/group -p wa -k identity -w /etc/passwd -p wa -k identity -w /etc/gshadow -p wa -k identity -w /etc/shadow -p wa -k identity -w /etc/security/opasswd -p wa -k identity
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄變更系統網路環境事件

ID	TWGCB-01-003-0150
說明	• 決定是否記錄變更系統網路環境之事件
檢測方法	執行下列指令： #sudo grep system-locale /etc/audit/audit.rules ・確認包含下列內容： -a exit,always -F arch=(b32或b64) -S sethostname -S setdomainname -k system-locale -w /etc/issue -p wa -k system-locale -w /etc/issue.net -p wa –k system-locale -w /etc/hosts -p wa -k system-locale -w /etc/sysconfig/network -p wa -k system-locale
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

記錄變更系統強制性存取控制(Mandatory access controls)事件

ID	TWGCB-01-003-0151
說明	• 決定是否記錄包含/etc/selinux目錄屬性變更，以及在此目錄內新增、刪除或修改檔案之事件
檢測方法	執行下列指令： #sudo grep MAC-policy /etc/audit/audit.rules 確認包含下列內容： -w /etc/selinux/ -p wa -k MAC-policy
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

記錄變更自主式存取控制(Discretionary access control)權限事件

ID	TWGCB-01-003-0152
說明	• 決定是否記錄變更自主式存取控制(Discretionary access control)權限之事件
檢測方法	執行下列指令： #sudo grep perm_mod /etc/audit/audit.rules 確認包含下列內容： -a always,exit -F arch=(b32或b64) -S chmod -S fchmod -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod -a always,exit -F arch=(b32或b64) -S chown -S fchown -S fchownat –S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod -a always,exit -F arch=(b32或b64) -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

記錄不成功的未經授權檔案存取

ID	TWGCB-01-003-0153
說明	• 決定是否記錄所有使用者未經授權存取檔案之行為
檢測方法	執行下列指令， #grep access /etc/audit/audit.rules 確認包含下列內容： -a always,exit -F arch=(b32或b64) -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access -a always,exit -F arch=(b32或b64) -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄特權指令使用情形

ID	TWGCB-01-003-0154
說明	• 決定是否記錄特權指令使用情形
檢測方法	• 執行下列指令，針對每個磁區(PART)的特權指令產生稽核規則： #find PART -xdev \(-perm -4000 -o -perm -2000 \) -type f | awk '{print \ "-a always,exit -F path=" $1 " -F perm=x –F auid>=500 -F auid!=4294967295 \ -k privileged" }' • 檢視/etc/audit/audit.rules檔案內容，確認是否已包含上述指令所產生之稽核規則
GCB設定值	啟用

- PART使用blkid查詢
- 上述指令待修正

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄資料匯出至媒體

ID	TWGCB-01-003-0155
說明	• 決定是否記錄資料匯出至媒體之事件
檢測方法	執行下列指令， #grep export /etc/audit/audit.rules 確認包含下列內容： -a always,exit -F arch=(b32或b64) -S mount -F auid>=500 -F auid!=4294967295 -k export
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄檔案刪除事件

ID	TWGCB-01-003-0156
說明	• 決定是否蒐集使用者利用unlink、unlinkat、rename或renameat等系統呼叫進行刪除檔案、移除檔案屬性、更換檔名或路徑等事件
檢測方法	執行下列指令， #grep delete /etc/audit/audit.rules 確認包含下列內容： -a always,exit –F arch=(b32或b64) -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄系統管理者活動

ID	TWGCB-01-003-0157
說明	• 決定是否記錄系統管理者活動
檢測方法	執行下列指令： #grep actions /etc/audit/audit.rules 確認包含下列內容： -w /etc/sudoers -p wa -k actions
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

記錄核心模組掛載與卸載事件

ID	TWGCB-01-003-0158
說明	• 決定是否記錄核心模組掛載與卸載事件
檢測方法	執行下列指令： #grep modules /etc/audit/audit.rules 確認包含下列內容： -w /sbin/insmod -p x -k modules -w /sbin/rmmod -p x -k modules -w /sbin/modprobe -p x -k modules -a always,exit -F arch=(b32或b64) -S init_module -S delete_module -k modules
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
auditd設定不變模式

ID	TWGCB-01-003-0159
說明	• 決定是否啟用auditd設定不變模式(Immutable mode)
檢測方法	執行下列指令，確認內容包含「-e 2」： #grep "^-e 2" /etc/audit/audit.rules
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核

記錄變更登入與登出資訊事件

ID	TWGCB-01-003-0160
說明	• 決定是否記錄嘗試變更登入與登出資訊之事件
檢測方法	執行下列指令： #grep logins /etc/audit/audit.rules 確認包含下列內容： -w /var/log/faillog -p wa -k logins -w /var/log/lastlog -p wa -k logins
GCB設定值	啟用

Linux伺服器安全基準

伺服主機安全性設定-安全性相關稽核事件設定-日誌與稽核
記錄程序與會談啟始資訊

ID	TWGCB-01-003-0161
說明	• 決定是否啟用程序(Proces)與會談(Session)啟始資訊記錄功能，以蒐集所有使用者登入、登出、重新開機或關機等資訊
檢測方法	執行下列指令： #grep session /etc/audit/audit.rules 確認包含下列內容： -w /var/run/utmp -p wa -k session -w /var/log/btmp –p wa -k session -w /var/log/wtmp -p wa -k session
GCB設定值	啟用

Linux伺服器安全基準

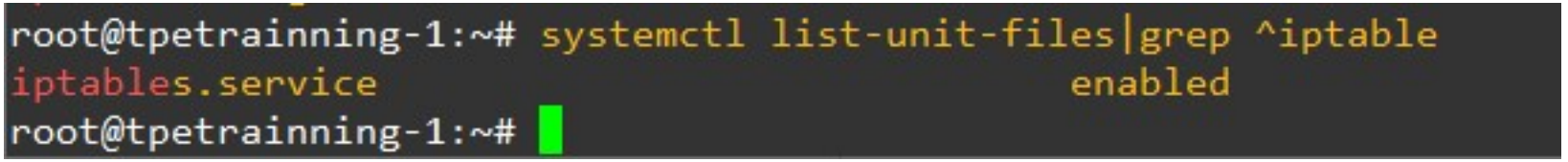
伺服主機安全性設定-安全性相關稽核事件設定
螢幕保護裝置設定(GNOME螢幕保護裝置逾時)

ID	TWGCB-01-003-0099
說明	• 這項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動
檢測方法	執行下列指令，確認idle_delay是否設為15： #gconftool-2 -R /apps/gnome-screensaver
GCB設定值	15分鐘

Linux伺服器安全基準

iptables服務

ID	TWGCB-01-003-0137
說明	• 決定是否啟用iptables服務
檢測方法	• 執行下列指令，確認所有執行層級皆設為啟用： #systemctl list-unit-files | grep ^iptables
GCB設定值	啟用



INPUT與FORWARD防火牆規則鏈的預設規則

ID	TWGCB-01-003-0138
說明	• 決定是否變更iptables內建之INPUT與FORWARD防火牆規則鏈的預設規則
檢測方法	• 執行下列指令：#cat /etc/sysconfig/iptables 確認etc/sysconfig/iptables檔案是否包含下列內容： *filter :INPUT DROP [0:0] :FORWARD DROP [0:0]
GCB設定值	DROP

IP轉送

ID	TWGCB-01-003-0121
說明	• 決定是否啟用IP轉送(Forwarding)功能
檢測方法	• 執行下列指令，確認net.ipv4.ip_forward是否設為0： sysctl net.ipv4.ip_forward
GCB設定值	停用(0)

所有網路介面傳送ICMP重新導向封包

ID	TWGCB-01-003-0122
說明	• 決定是否允許所有網路介面傳送ICMP重新導向(Redirect)封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.send_redirects是否設為0： #sysctl net.ipv4.conf.all.send_redirects
GCB設定值	停用(0)

預設網路介面傳送ICMP重新導向封包

ID	TWGCB-01-003-0123
說明	• 決定是否允許預設網路介面傳送ICMP重新導向(Redirect)封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.default.send_redirects是否設為0： #sysctl net.ipv4.conf.default.send_redirects
GCB設定值	停用(0)

所有網路介面接受安全的ICMP重新導向封包

ID	TWGCB-01-003-0124
說明	• 決定所有網路介面是否允許接受安全的ICMP重新導向封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.secure_redirects是否設為0： #sysctl net.ipv4.conf.all.secure_redirects
GCB設定值	停用(0)

預設網路介面接受安全的ICMP重新導向封包

ID	TWGCB-01-003-0125
說明	• 決定預設網路介面是否允許接受安全的ICMP重新導向封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.default.secure_redirects是否設為0： #sysctl net.ipv4.conf.default.secure_redirects
GCB設定值	停用(0)

所有網路介面接受ICMP重新導向封包

ID	TWGCB-01-003-0126
說明	• 決定所有網路介面是否允許接受ICMP重新導向封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.accept_redirects是否設為0： #sysctl net.ipv4.conf.all.accept_redirects
GCB設定值	停用(0)

預設網路介面接受ICMP重新導向封包

ID	TWGCB-01-003-0127
說明	• 決定預設網路介面是否允許接受ICMP重新導向封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.default.accept_redirects是否設為0：： #sysctl net.ipv4.conf.default.accept_redirects
GCB設定值	停用(0)

所有網路介面接受來源路由封包

ID	TWGCB-01-003-0128
說明	• 決定所有網路介面是否允許接受來源路由封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.accept_source_route是否設為0： #sysctl net.ipv4.conf.all.accept_source_route
GCB設定值	停用(0)

預設網路介面接受來源路由封包

ID	TWGCB-01-003-0129
說明	• 決定預設網路介面是否允許接受來源路由封包
檢測方法	• 執行下列指令，確認net.ipv4.conf.default.accept_source_route是否設為0： #sysctl net.ipv4.conf.default.accept_source_route
GCB設定值	停用(0)

忽略偽造的ICMP錯誤訊息

ID	TWGCB-01-003-0130
說明	• 決定是否忽略偽造的ICMP錯誤訊息，以避免系統遭受ICMP攻擊
檢測方法	• 執行下列指令，確認 net.ipv4.icmp_ignore_bogus_error_responses是否設為1： #sysctl net.ipv4.icmp_ignore_bogus_error_responses
GCB設定值	啟用(1)

不回應ICMP廣播要求

ID	TWGCB-01-003-0131
說明	• 決定是否不回應ICMP廣播要求，以防遭受ICMP攻擊
檢測方法	• 執行下列指令，確認net.ipv4.icmp_echo_ignore_broadcasts是否設為1： #sysctl net.ipv4.icmp_echo_ignore_broadcasts
GCB設定值	啟用(1)

紀錄可疑封包

ID	TWGCB-01-003-0132
說明	• 決定是否記錄如偽造封包、來源路由封包或重新導向等可疑封包，以協助系統管理者早期發現系統遭受攻擊跡象
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.log_martians是否設為1： #sysctl net.ipv4.conf.all.log_martians
GCB設定值	啟用(1)

所有網路介面啟用逆向路徑過濾功能

ID	TWGCB-01-003-0133
說明	• 決定是否啟用逆向路徑過濾(Reverse path filtering)功能
檢測方法	• 執行下列指令，確認net.ipv4.conf.all.rp_filter是否設為1： #sysctl net.ipv4.conf.all.rp_filter
GCB設定值	啟用(1)

預設網路介面啟用逆向路徑過濾功能

ID	TWGCB-01-003-0134
說明	• 決定是否啟用逆向路徑過濾(Reverse path filtering)功能
檢測方法	• 執行下列指令，確認net.ipv4.conf.default.rp_filter是否設為1： #sysctl net.ipv4.conf.default.rp_filter
GCB設定值	啟用(1)

TCP SYN cookies

ID	TWGCB-01-003-0135
說明	• 決定是否啟用TCP SYN cookies功能
檢測方法	• 執行下列指令，確認net.ipv4.tcp_syncookies是否設為1： #sysctl net.ipv4.tcp_syncookies
GCB設定值	啟用(1)

無線網路介面卡

ID	TWGCB-01-003-0136
說明	• 決定是否停用無線網路介面卡
檢測方法	• 執行下列指令，確認是否不包含無線網路介面卡： #cat /proc/net/dev 或 #ifconfig –a
GCB設定值	停用(不含wlan或wifi等)