資訊安全與管控

kali Tool

- nmap使用指令
- OPENVAS(GVM) 使用說明
- 簡易工具與指令
- 暴力密碼破解工具

nmap□□□

□□□□□

```
nmap -v www.hinet.net
```

```
nmap -A ip□□(□□□□port□□□□□□□□□□□□□)
```

EX:□-A -Pn□□

```
nmap -A -Pn {IP}
```

```
Nmap scan report for [redacted]
Host is up (0.018s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Apache httpd 2.4.27 ((Win64) OpenSSL/1.1.0f PHP/5.6.31)
|_http-server-header: Apache/2.4.27 (Win64) OpenSSL/1.1.0f PHP/5.6.31
|_http-title: \xAAF\xABn\xAC\xEC\xA4j\xAE\xD5\xB6\xE9\xB8\xEA\xB0T\xA8t\xB2\xCE
| http-robots.txt: 2 disallowed entries
|_/ /*.jpg$
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
443/tcp   open  ssl/http           Apache httpd 2.4.27 ((Win64) OpenSSL/1.1.0f PHP/5.6.31)
|_http-title: \xAAF\xABn\xAC\xEC\xA4j\xAE\xD5\xB6\xE9\xB8\xEA\xB0T\xA8t\xB2\xCE
| ssl-cert: Subject: commonName=[redacted]
| Subject Alternative Name: [redacted]
| Not valid before: 2024-08-16T06:26:59
|_Not valid after:  2025-08-27T15:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| http-robots.txt: 2 disallowed entries
|_/ /*.jpg$
|_http-server-header: Apache/2.4.27 (Win64) OpenSSL/1.1.0f PHP/5.6.31
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=SERVER04
| Not valid before: 2024-12-28T04:59:51
|_Not valid after:  2025-06-29T04:59:51
|_ssl-date: 2025-05-02T08:44:37+00:00; +1s from scanner time.
49154/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SERVER04, NetBIOS user: <unknown>, NetBIOS MAC: [redacted] (VMware)
| smb2-time:
|   date: 2025-05-02T08:43:57
|_  start_date: 2025-03-13T04:12:50
| smb2-security-mode:
|   2:1:0:
```

□□□

```
nmap 192.168.0.* --exclude 192.168.0.100
```

□□□□□

```
nmap -iL hostlist.txt --excludefile excludelist.txt
```

檢測是否有使用防火牆(不會完成3手交握)

```
nmap -sA scanme.nmap.org
```

掃描有防火牆的主機

```
nmap -PN scanme.nmap.org
```

偵測主機是否開機(ping scan)

```
nmap -sP 140.115.35.0/24
```

```
nmap -F www.hinet.net
#快速掃描 也可以使用-T5, 預設-T3
```

按照port做掃描

```
nmap -p 80,443 192.168.1.1
nmap -p 80-200 192.168.1.1
```

使用tcp掃描

```
nmap -p T:80 192.168.1.1
```

使用udp掃描

```
nmap -p U:53 192.168.1.1
```

最常用的10port

```
nmap --top-ports 10 192.168.1.1
```

綜合掃描

```
nmap -sS -P0 -sV -O 192.168.56.102
param:
-sS: Scan Syn
-sV: Determine OS Version
-P0: Protocol Scan
-O : Operation System
```

script scan

```
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
```

驗證所有使用的TLS版本

```
nmap --script ssl-enum-ciphers -p 443 {url}
```

如果要驗證整個網段，可以先產生出txt檔。比如10.0.0.0/16的tls

```
echo 10.0.{1..254}.{1..254} >> iplist.txt
```

建立一個sh檔（此例子只檢查tls1.0-1.如需要檢查不一樣的加密方式可以自行增減）

```
#!/bin/bash

IPLIST=($(cat iplist.txt))
TLS_VER=(TLSv1.0 TLSv1.1 TLSv1.2)
SCAN_PORT="443"
NMAP_OPS="--host-timeout 3000ms --max-rtt-timeout 3000ms --script ssl-enum-ciphers -p ${SCAN_PORT}"
OUTPUT="output.csv"

for (( i = 0; i < ${#IPLIST[@]}; i++ )); do
  SUP_TLS=$(nmap $NMAP_OPS ${IPLIST[i]} | egrep "${TLS_VER[0]}|${TLS_VER[1]}|${TLS_VER[2]}" | cut -c 5-11)

  if [[ ! -z $SUP_TLS ]]; then
    echo -ne "\n${IPLIST[i]}" >> $OUTPUT

    for (( j = 0; j < ${#SUP_TLS[@]}; j++ )); do
      echo -n ",${SUP_TLS[@]}" >> $OUTPUT
```

```
    done
  fi

  unset SUP_TLS
done
```

參考網址

用 nmap 驗證支援的 TLS 版本和 Ciphers (Mr.沙先生)

OPENVAS(GVM) 使用說明

openvas安裝

Kali安裝

```
sudo apt install gvm
```

備註: 其他**linux**版本請參閱官方安裝文件

https://greenbone.github.io/docs/latest/22.4/source-build/index.html

人家整理好的debian快速安裝方式

https://github.com/Kastervo/OpenVAS-Installation

初始化gvm

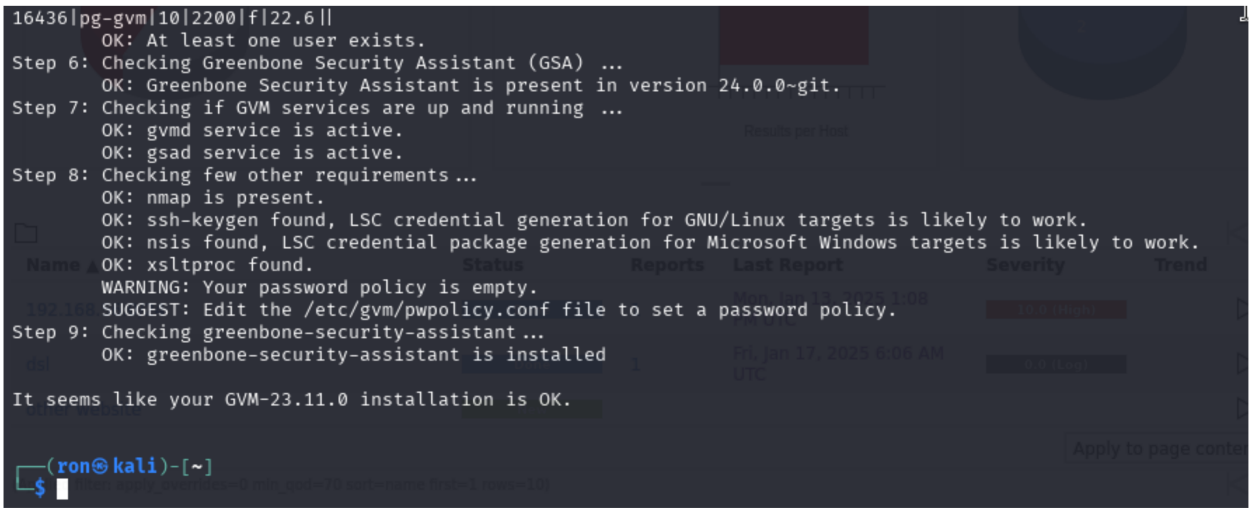
```
sudo gvm-setup
```

備註: 完成後會自動產生新密碼，如果忘記可用以下指令修改。

```
sudo runuser -u _gvm -- gvmd --user=admin --new-password=password
```

檢查安裝

```
sudo gvm-check-setup
```



最後Seems like your GVM-xx.xx.xx installation is OK.代表有安裝完成。

啟用gvm

```
sudo gvm-start
```

備註: 這個程式會自動開啟**gsad(GreenBone Security Assistant daemon)**、**gvmd(greenbone Vulnerability M daemon)**跟**opsd-openvas**三個服務，完成後也會自動開啟遊覽器。

注意!！第一次啟用**gvm**後要等程式將資料完整的寫到資料庫後才可以正常運作，需要時間是電腦效能可能幾十分鐘到幾小時。

預設網址: https://127.0.0.1:9392

停止gvm

```
sudo gvm-stop
```

修改服務IP跟Port

```
sudo vi /usr/lib/systemd/system/gasd.service
```

將**-listen** 更改[redacted]則可以更改成想要的port，完成厚重啟服務。

更新資料庫

```
sudo greenbone-feed-sync
```

也可以

```
sudo greenbone-feed-sync --type nvt
sudo greenbone-feed-sync --type scap
```

```
sudo greenbone-feed-sync --type cert
```

備註：也可以使用**cron**讓資料庫定期更新。

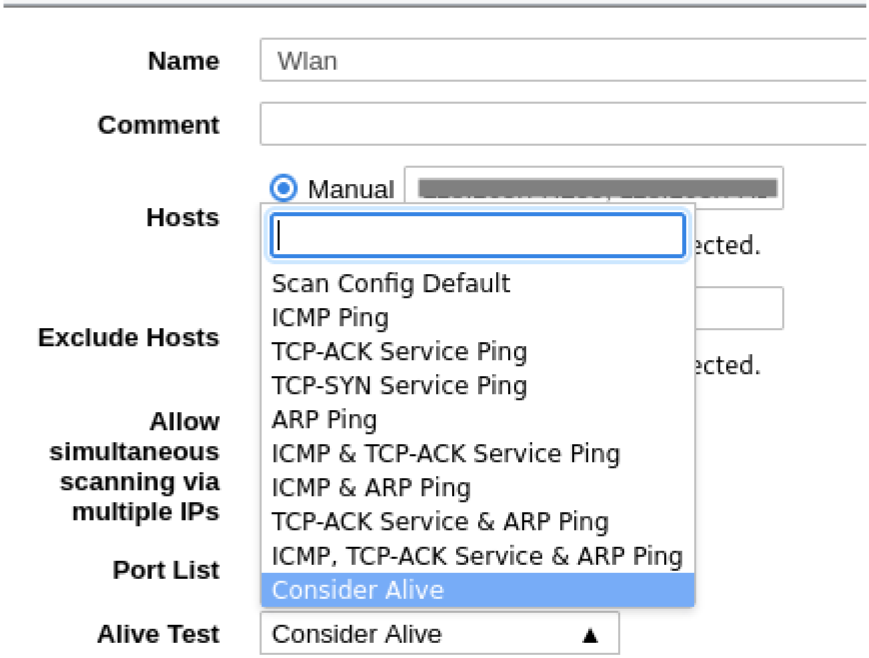
重置GVM

```
sudo -u _gvm gvmd --rebuild-gvmd-data=all
```

其他

如果安裝openvas的裝置使用外部ip直接對其他實體（外部）ip做弱點掃描時會出現掃不出任何結果的狀況時，

將Alive Test□**Scan config Default**□**Consider Alive**就可以了。



更□□□□□□□□1(Database is wrong Version)

顯示狀態如下

```
┌──(ron㉿cc140-87)-[~]
└─$ sudo systemctl status gvmd.service
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: activating (start) since Wed 2025-04-09 13:25:28 CST; 38s ago
        Job: 1660
 Invocation: 80b19be4686a4a329bc4609347cb1fd9
       Docs: man:gvmd(8)
    Process: 2595 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
      Tasks: 0 (limit: 19043)
     Memory: 4K (peak: 5.8M)
        CPU: 17ms
     CGroup: /system.slice/gvmd.service

Apr 09 13:25:28 cc140-87 systemd[1]: gvmd.service: Scheduled restart job, restart counter is at 1.
Apr 09 13:25:28 cc140-87 systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Apr 09 13:25:28 cc140-87 gvmd[2595]: md   main:MESSAGE:2025-04-09 05h25.28 utc:2595:    Greenbone Vulnerability Manager version 25.1.3 (DB revision 258)
Apr 09 13:25:28 cc140-87 systemd[1]: gvmd.service: Can't open PID file '/run/gvmd/gvmd.pid' (yet?) after start: No such file or directory
Apr 09 13:25:28 cc140-87 gvmd[2597]: md manage:MESSAGE:2025-04-09 05h25.28 utc:2597: check_db_versions: database version of database: 256
Apr 09 13:25:28 cc140-87 gvmd[2597]: md manage:MESSAGE:2025-04-09 05h25.28 utc:2597: check_db_versions: database version supported by manager: 258
Apr 09 13:25:28 cc140-87 gvmd[2597]: md   main:CRITICAL:2025-04-09 05h25.28 utc:2597: gvmd: database is wrong version
Apr 09 13:25:28 cc140-87 gvmd[2597]: md   main:CRITICAL:2025-04-09 05h25.28 utc:2597: gvmd: Your database is too old for this version of gvmd.
Apr 09 13:25:28 cc140-87 gvmd[2597]: md   main:CRITICAL:2025-04-09 05h25.28 utc:2597: gvmd: Please migrate to the current data model.
Apr 09 13:25:28 cc140-87 gvmd[2597]: md   main:CRITICAL:2025-04-09 05h25.28 utc:2597: gvmd: Use a command like this: gvmd --migrate
```

□□

```
gvmd --migrate
```

□□□□"root" does not exist□

```
┌──(ron㉿cc140-87)-[~]
└─$ sudo gvmd --migrate

(gvmd:4844): md manage-WARNING **: 13:29:50.001: sql_open: PQconnectPoll failed

(gvmd:4844): md manage-WARNING **: 13:29:50.001: sql_open: PQerrorMessage (conn): connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:  role "root" does not exist


(gvmd:4844): md manage-WARNING **: 13:29:50.001: init_manage_open_db: sql_open failed
```

□□

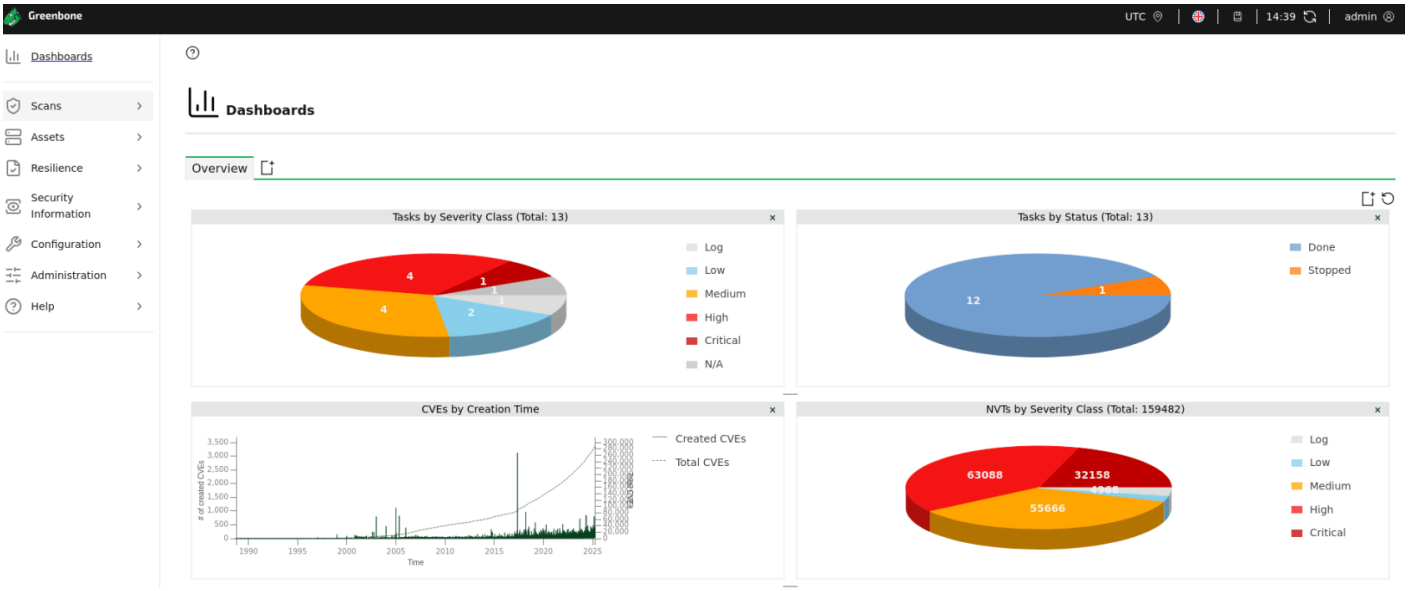
```
gvm-setup solve
```

□□□□□□□

```
┌──(ron㉿cc140-87)-[~]
└─$ sudo gvm-setup solve

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
NOTICE:  role "_gvm" has already been granted membership in role "dba" by role "postgres"
GRANT ROLE
[i] Extension uuid-ossp already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
md    main:MESSAGE:2025-04-09 05h48.46 utc:14414:    Greenbone Vulnerability Manager version 25.1.3 (DB revision 258)
md    main:    INFO:2025-04-09 05h48.46 utc:14414:    Migrating database.
md    main:    INFO:2025-04-09 05h48.46 utc:14414:    Migrating to 257
md    main:    INFO:2025-04-09 05h48.46 utc:14414:    Migrating to 258
md    main:MESSAGE:2025-04-09 05h48.46 utc:14414: Migrating SCAP database
md manage:    INFO:2025-04-09 05h48.46 utc:14414: Reinitialization of the SCAP database necessary
md manage:WARNING:2025-04-09 05h48.47 utc:14414: update_scap: Full rebuild requested, resetting SCAP db
md manage:    INFO:2025-04-09 05h48.47 utc:14414: update_scap: Updating data from feed
md manage:    INFO:2025-04-09 05h48.47 utc:14414: Updating CPEs
md manage:    INFO:2025-04-09 05h48.47 utc:14414: Updating /var/lib/gvm/scap-data/nvd-cpes.json.gz
md manage:    INFO:2025-04-09 05h49.43 utc:14414: Updating CPE refs ...
md manage:    INFO:2025-04-09 05h50.02 utc:14414: Updating CPE match strings from /var/lib/gvm/scap-data/nvd-cpe-matches.json.gz
md manage:    INFO:2025-04-09 05h55.11 utc:14414: Updating CVEs
md manage:    INFO:2025-04-09 05h55.11 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2003.json.gz
md manage:    INFO:2025-04-09 05h57.02 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2001.json.gz
md manage:    INFO:2025-04-09 05h57.04 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2019.json.gz
md manage:    INFO:2025-04-09 05h57.35 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2022.json.gz
md manage:    INFO:2025-04-09 05h58.41 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2008.json.gz
md manage:    INFO:2025-04-09 05h58.47 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2025.json.gz
md manage:    INFO:2025-04-09 05h58.56 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2024.json.gz
md manage:    INFO:2025-04-09 06h00.24 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2006.json.gz
md manage:    INFO:2025-04-09 06h00.29 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2012.json.gz
md manage:    INFO:2025-04-09 06h00.47 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2007.json.gz
md manage:    INFO:2025-04-09 06h00.52 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2002.json.gz
md manage:    INFO:2025-04-09 06h00.54 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2016.json.gz
md manage:    INFO:2025-04-09 06h01.20 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2020.json.gz
md manage:    INFO:2025-04-09 06h02.02 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2010.json.gz
md manage:    INFO:2025-04-09 06h02.13 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2013.json.gz
md manage:    INFO:2025-04-09 06h02.34 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2015.json.gz
md manage:    INFO:2025-04-09 06h02.54 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2018.json.gz
md manage:    INFO:2025-04-09 06h03.19 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2011.json.gz
md manage:    INFO:2025-04-09 06h03.43 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2009.json.gz
md manage:    INFO:2025-04-09 06h03.57 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2004.json.gz
md manage:    INFO:2025-04-09 06h04.02 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2000.json.gz
md manage:    INFO:2025-04-09 06h04.04 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2005.json.gz
md manage:    INFO:2025-04-09 06h04.10 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2021.json.gz
md manage:    INFO:2025-04-09 06h05.09 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-1999.json.gz
md manage:    INFO:2025-04-09 06h05.12 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2017.json.gz
md manage:    INFO:2025-04-09 06h06.56 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2014.json.gz
md manage:    INFO:2025-04-09 06h08.13 utc:14414: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2023.json.gz
md manage:    INFO:2025-04-09 06h09.53 utc:14414: update_epss_scores: EPSS scores file '/var/lib/gvm/scap-data/epss-scores-current.json' not found
```

□□□□□□

□□□gvm□□□□□□□□□□□□□□□□



□□□

https://greenbone.github.io/docs/latest/22.4/kali/index.html

https://www.greenbone.net/en/documents/

https://github.com/greenbone/

https://community.greenbone.net/getting-started/greenbone-community-edition-via-linux-distribution-packages/

https://forum.greenbone.net/t/your-database-is-too-old-for-this-version-of-gvmd/20812

簡易工具與指令

nslookup

可以查詢網域所對應的ip

```
nslookup 2022.4inlibra.com {可指定使用的dns}
```

```
ron@ubuntu2:~$ nslookup 2022.4inlibra.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   2022.4inlibra.com
Address: 118.163.77.237
```

whois

可以得知域名註冊、Dns伺服器等相關資訊

whatweb

除網域登記者、ip等等網域資料外，還有網站的相關內容分析，如使用何種語言、網頁伺服器還有版本等等

暴力密碼破解工具

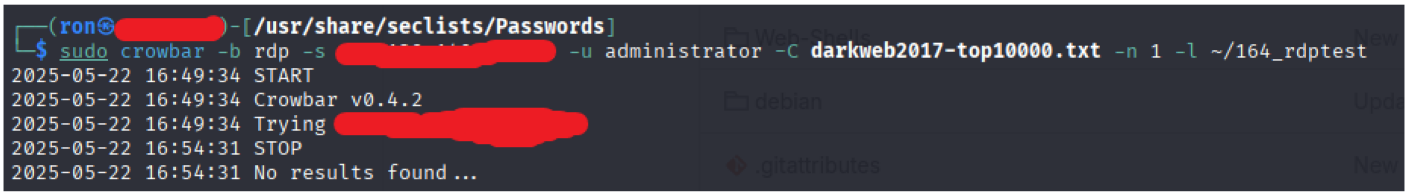
crowbar

安裝 (kali)

```
sudo apt install crowbar
```

使用方式

```
crowbar -b {ssh,ftp...} -u {username} -c {password} -n {session number} -l {logfile}
#-u可以改成-U 用使用者txt名單, -c也可以變成-C 使用密碼txt名單
```



備註: 注意如果只掃一個ip也要輸入/32, 不然會顯示錯誤。