

Greenbone X 滲透測試平台

免責聲明

本文檔中的資訊僅供參考之用，不應被視為專業建議。在採取任何基於本文檔的行動之前，讀者應該進行獨立的評估和驗證。本文檔的作者或提供者不承擔因使用或依賴本文檔中的任何資訊而導致的任何直接、間接、偶發、特殊或後續損害的責任。

請注意，本文檔中提到的任何外部鏈接或參考資源都是在發布時認為可靠，但作者或提供者無法保證這些資源的持續可訪問性或準確性。對於任何外部鏈接的內容，作者或提供者不承擔責任。

本文檔的內容可能會隨時間而變更，作者或提供者保留隨時更新或更改資訊的權利，無需提前通知。

簡介

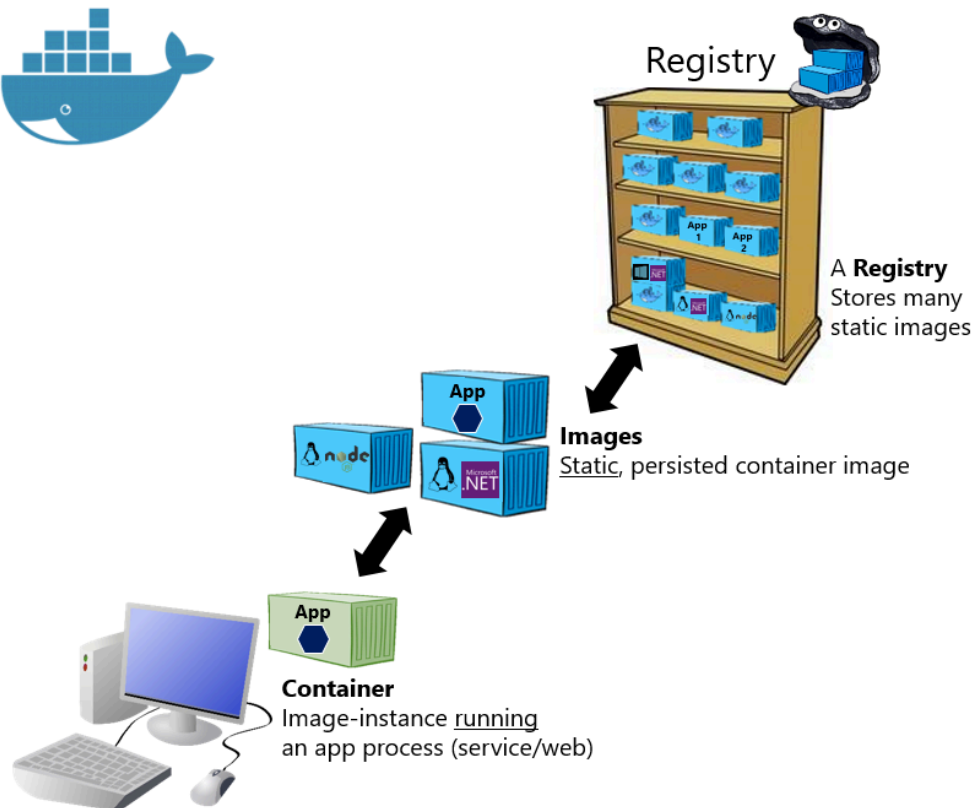
- 課程目標
 - Docker 的基本操作
 - Greenbone 的基本操作
 - 滲透測試的基本操作

Docker 介紹與安裝

Docker 是一個開源的容器化平台，它允許開發者將應用程式及其依賴項打包到一個容器中。這個容器可以在任何支持Docker的系統上運行，確保了應用程式在不同環境間的一致性和可移植性。這對於開發、測試和生產環境的一致性提供了極大的便利。

Docker 架構

Basic taxonomy in Docker



Hosted Docker Registry

Docker Trusted Registry on-prem.

On-premises
(‘n’ private organizations)

Docker Hub Registry

Docker Trusted Registry on-cloud

Azure Container Registry

AWS Container Registry

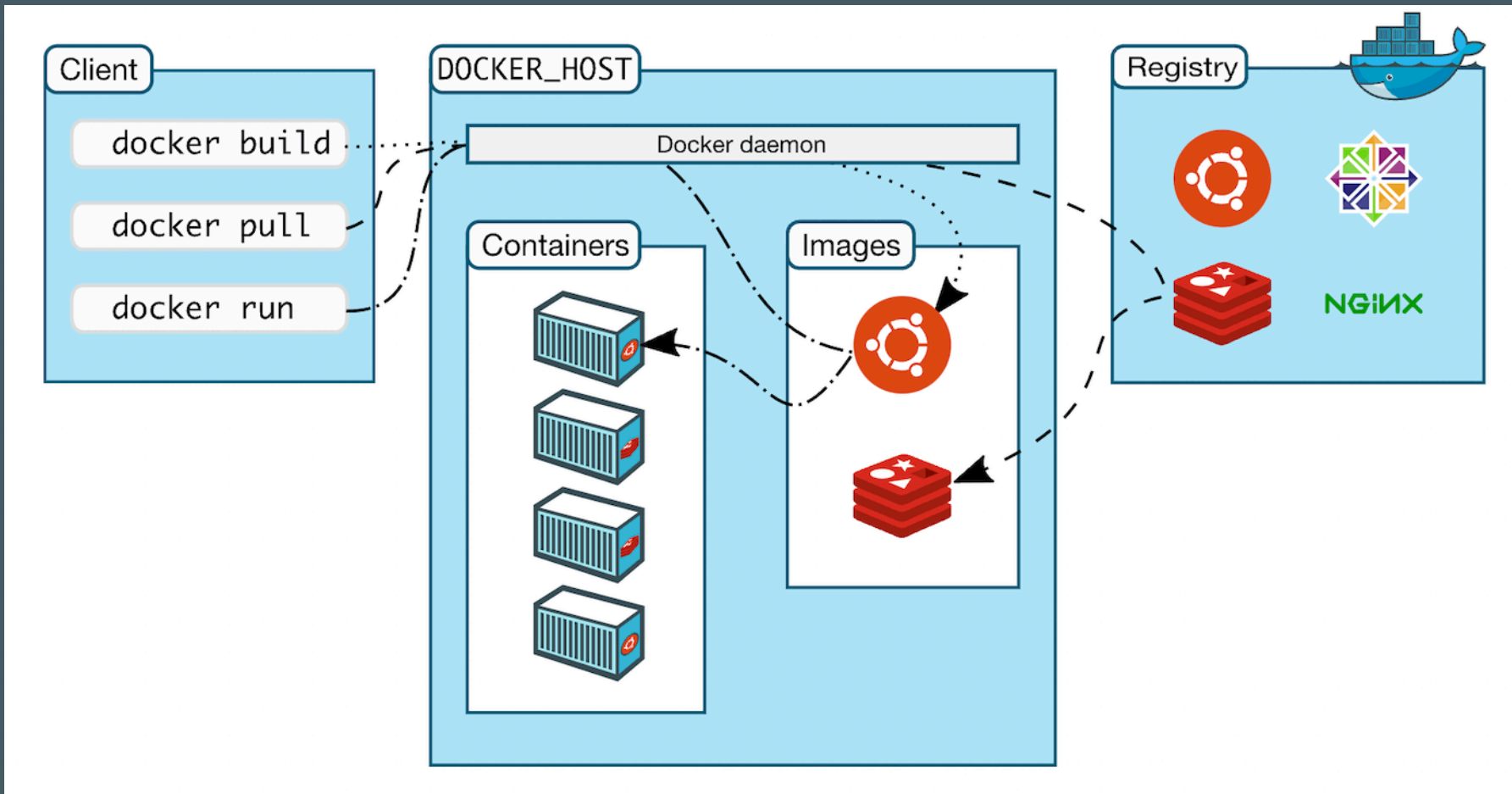
Public Cloud
(specific vendors)

Google Container Registry

Quay Registry

Other Cloud

Docker Overview



Docker 安裝

- Windows

- [Docker Desktop](#)

- Mac

- [Docker Desktop](#)

- Linux

- ```
sudo apt-get update
curl -sSL https://get.docker.com | sh
sudo apt install -y docker-compose
```

# Greenbone 介紹與安裝

Greenbone Security Manager (GSM) 是一款強大的漏洞管理解決方案，用於識別、管理和減輕網絡安全風險。它是基於開源漏洞管理工具 OpenVAS 的商業版本，提供全面的漏洞掃描、網絡監測以及報告功能。





## 為什麼使用Greenbone?

- **全面的安全評估**：提供廣泛的漏洞掃描覆蓋，從網絡服務到應用程序層面的弱點。
- **持續監控**：能夠持續監控網絡狀態，即時發現新的或已知的漏洞。
- **易於管理的報告功能**：生成詳細的安全報告，幫助分析風險並規劃糾正措施。

# Greenbone 安裝

```
git clone https://github.com/hibana2077/hack2024_spring.git
cd hack2024_spring
cd greenbone
```

## Windows

```
docker-compose up -d
```

## Linux

```
sudo docker-compose up -d
```

# Greenbone 登入

如果你是安裝在本機，請使用以下網址開啟 Greenbone。

- 網址：<http://localhost:9392>

如果是遠端機器，你需要把 `localhost` 換成遠端機器的IP。

預設帳號密碼為：  
admin / admin



## Greenbone

### Warning: Connection unencrypted

The connection to this GSA is not encrypted, allowing anyone listening to the traffic to steal your credentials.

Please configure a TLS certificate for the HTTPS service or ask your administrator to do so as soon as possible.

### Sign in to your account

Username

---

Password

---

Sign In

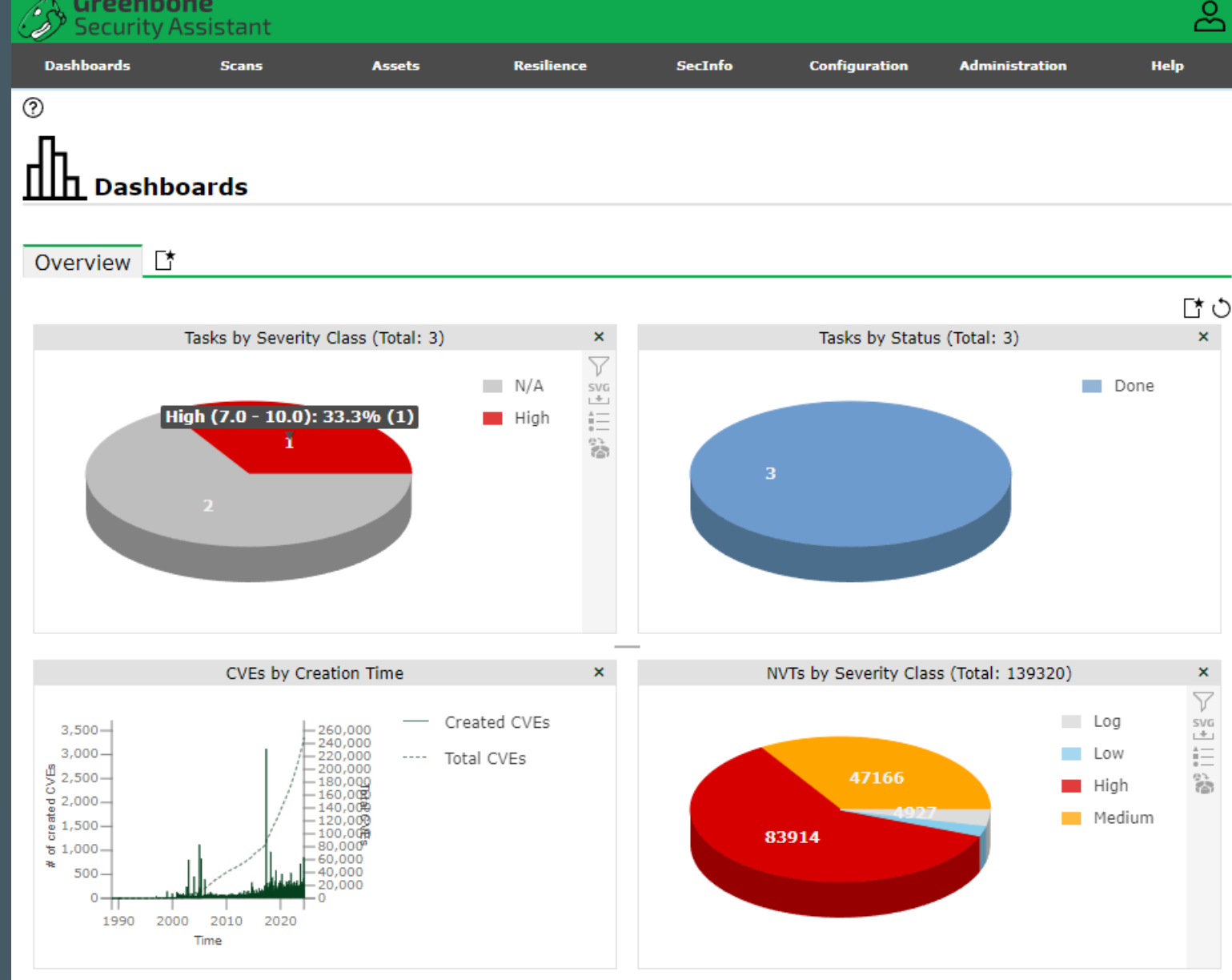


# Greenbone 基礎介紹

- **Dashboard**：網絡狀態概覽
- **Scans**：漏洞掃描
- **Assets**：網絡設備
- **Administration**：管理設定

# Greenbone Dashboard

- Tasks by Severity Class
- Tasks by Status
- CVEs by Creation Time
- NVTs by Severity Class



# Greenbone Scans

- **Tasks** : 掃描任務
- **Reports** : 報告

# Greenbone Assets

- **Hosts** : 主機
- **Operating Systems** : 作業系統
- **TLS Certificates** : TLS 憑證

# Greenbone Administration

- **Users** : 使用者
- **Feed Status** : 資料庫狀態



# 漏洞資料庫簡短介紹

## **NVTs : Network Vulnerability Tests**

NVTs 是一組用於檢測網絡設備和系統中已知漏洞的測試。這些測試通常由自動化的安全工具如OpenVAS進行，能夠檢查網絡中的各種設備是否容易受到已知攻擊的影響。NVTs 是維護網絡安全健康的重要工具，能夠提供即時的漏洞評估和管理。

# 漏洞資料庫簡短介紹

## **CVEs : Common Vulnerabilities and Exposures**

CVEs 是一個廣泛認可的信息安全漏洞和曝光資料庫。每個CVE條目提供了一個標準化的識別號，用於公開分享全球範圍內的信息安全漏洞。這個系統使得安全專家可以在討論、管理和解決安全問題時共享資訊，並確保業界對特定漏洞有一致的理解。

# 漏洞資料庫簡短介紹

## **CPEs : Common Platform Enumeration**

CPEs 是一套標準化方法，用於識別和枚舉應用程式、作業系統以及硬件設備中的漏洞。CPE提供了一個統一的命名架構，使得安全專家可以準確地描述系統中存在的特定產品和版本，從而在探討漏洞時提高溝通的清晰度和效率。

# Vulnhub

[VulnHub](#) 是一個提供實際安全漏洞練習機會的平台，專門為安全愛好者、教育者和IT安全專家設計。它提供了大量可自由下載的虛擬機映像，這些映像故意設計有安全漏洞，以便於進行滲透測試和安全訓練。



# 功能和用途

- **實戰訓練**：VulnHub 提供的虛擬機映像含有各種漏洞，用戶可以在一個安全的環境中練習滲透技術。
- **教育目的**：學校和培訓機構常用VulnHub來教學生實際的安全技巧，因為它可以模擬真實世界的安全挑戰。
- **技能提升**：對於有經驗的安全專業人員，VulnHub提供一個平台來鍛煉和提升解決複雜漏洞的能力。

# Vulhub

“ Vulhub是一個基於docker和docker-compose的漏洞環境集合，進入對應目錄並執行一條語句即可啟動一個全新的漏洞環境，讓漏洞覆現變得更加簡單，讓安全研究者更加專注於漏洞原理本身。

-- VulnHub 官網

”

- [VulnHub](https://vulnhub.com/)



# Vulhub 下載

```
Use wget to download the repository(bc. it's faster than git clone)
wget https://github.com/vulhub/vulhub/archive/master.zip -O vulhub-master.zip
unzip vulhub-master.zip
```

```
Entry vulnerability directory
cd vulhub-master
```

# 實戰演練

這次以 `CVE-2020-17526` 為例，進行滲透測試。



# 漏洞描述

“ Incorrect Session Validation in Apache Airflow Webserver versions prior to 1.10.14 with default config allows a malicious airflow user on site A where they log in normally, to access unauthorized Airflow Webserver on Site B through the session from Site A. This does not affect users who have changed the default value for `[webserver] secret_key` config. -- [CVE-2020-17526](#) ”

# 講人話

“ 我忘記改配置文件了！ ”

就是在Apache Airflow Webserver的某些版本中，如果保持默認配置，當一個惡意用戶在一個站點（ Site A ）正常登錄後，他可以利用同一個會話（ session ）信息在另一個站點（ Site B ）進行未授權的訪問。這是因為默認的[webserver] secret\_key配置沒有被修改，導致跨站點的會話管理存在安全漏洞。

# 啟動漏洞環境

```
cd vulhub/airflow/CVE-2020-17526
```

Linux 環境要加上 `sudo`

```
docker compose run airflow-init
docker compose up -d
```

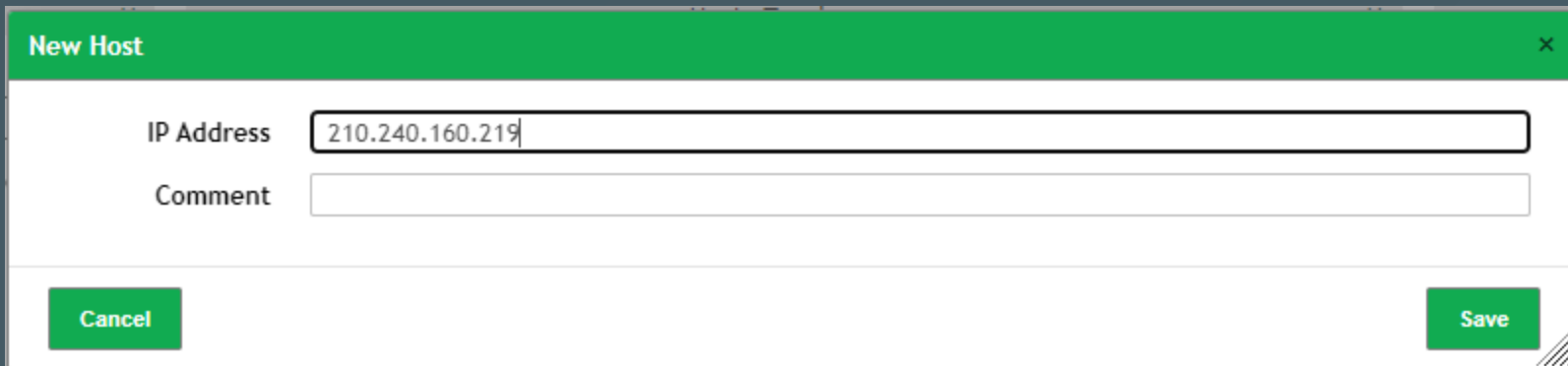
# 漏洞掃描

- 使用Greenbone掃描漏洞

執行此實驗時，請確保你在台東大學校園網路中，否則可能被視為攻擊行為。

# 建立 Asset

- 在Greenbone中建立一個新的Asset，用於掃描漏洞。
- IP : 210.240.160.219



New Host

IP Address 210.240.160.219

Comment

Cancel Save

# 建立 Target

New Target

Name

hack\_demo\_target

Comment

Hosts

☐ Manual

☐ From file 選擇檔案 未選擇任何檔案

☒ From host assets (1 hosts)

Exclude Hosts

☒ Manual

☐ From file 選擇檔案 未選擇任何檔案

Allow simultaneous scanning via multiple IPs

☒ Yes ☐ No

Port List

All IANA assigned TCP and

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

--

on port

22

Cancel

Save

# 建立 Task

New Task ×

Name

hack\_demo\_1

Comment

Scan Targets

hack\_demo\_target ▼

✎

Alerts

✎

Schedule

-- ▼

☐ Once

✎

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70

▲▼

%

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

▲▼

reports

Scanner

OpenVAS Default ▼

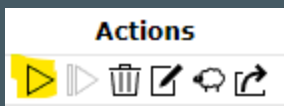
Scan Config

Full and fast ▼

Cancel









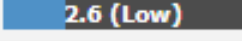


Save

# 開始掃描





# 掃描結果 I

| Vulnerability                                                                                                                                                                               |  | Severity ▼                                                                          | QoD  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------|
| <a href="#">Synology DiskStation Manager (DSM) 7.0.x &lt; 7.0.1-42218-6, 7.1.x &lt; 7.1.1-42962-3 Multiple Vulnerabilities (Synology-SA-22:23) - Remote Known Vulnerable Versions Check</a> |  |  | 80 % |
| <a href="#">Synology DiskStation Manager (DSM) &lt; 7.2-64561 ACE Vulnerability (Synology-SA-24:01)</a>                                                                                     |  |  | 80 % |
| <a href="#">Synology DiskStation Manager (DSM) &lt; 7.2.1-69057-2 Open Redirect Vulnerability (Synology-SA-24:02) - Remote Known Vulnerable Versions Check</a>                              |  |  | 80 % |
| <a href="#">TCP Timestamps Information Disclosure</a>                                                                                                                                       |  |  | 80 % |
| <a href="#">ICMP Timestamp Reply Information Disclosure</a>                                                                                                                                 |  |  | 80 % |

# 掃描結果 II

## Summary

Synology DiskStation Manager (DSM) is prone to multiple vulnerabilities.

## Detection Result

Installed version: 7.1-42661  
Fixed version: 7.1.1-42962-3

## Product Detection Result

Product [cpe:/h:synology:ds418](#)

Method [Synology NAS / DiskStation Manager \(DSM\) Detection Consolidation \(OID: 1.3.6.1.4.1.25623.1.0.170202\)](#)

Log [View details of product detection](#)

## Insight

Multiple vulnerabilities reported by PWN2OWN TORONTO 2022 have been addressed.

- Claroty Research was able to execute a chain of 3 bugs (2 missing authentication for critical function and an authentication bypass) attack against the Synology DiskStation DS920+
- ASU SEFCOM was able to execute their OOB Write attack against the Synology DiskStation DS920+ to gain code execution

## Detection Method


Checks if a vulnerable version is present on the target host.

# 掃描結果 III

## Affected Software/OS

Synology DSM versions 7.0.x prior to 7.0.1-42218-6 and 7.1.x prior to 7.1.1-42962-3.

## Solution

**Solution Type:**  Vendorfix

Update to firmware version 7.0.1-42218-6, 7.1.1-42962-3 or later.

## References

CVE [CVE-2022-45188](#)

CERT [DFN-CERT-2023-2228](#)  
[DFN-CERT-2023-1134](#)  
[DFN-CERT-2023-0745](#)  
[DFN-CERT-2022-2797](#)

Other [https://www.synology.com/en-global/security/advisory/Synology\\_SA\\_22\\_23](https://www.synology.com/en-global/security/advisory/Synology_SA_22_23)  
<https://www.zerodayinitiative.com/blog/2022/12/5/pwn2own-toronto-2022-day-one-results>  
<https://rushbnt.github.io/bug%20analysis/netatalk-0day/>  
<https://netatalk.io/3.1/ReleaseNotes3.1.15>

## [CVE-2022-45188](#)

# 生成報告

Report: Wed, May 15, 2024 1:28 PM UTC Done

Information **Results** (5 of 77) Hosts (1 of 1) Ports (0 of 12) Applications (5 of 5) Operating Systems (1 of 1)

Compose Content for Scan Report ×

Results Filter

Include ☒ Notes ☒ Overrides ☒ TLS Certificates

Report Format

☐ Store as default

Cancel OK

# 結論

- Docker 的基本概念與操作
- 漏洞資料庫的認識
- Greenbone 的基礎操作

# 參考資源

- [Docker Documentation](#)
- [Greenbone Community Edition](#)
- [VulnHub](#)
- [CVE-2020-17526](#)

結束