第五十一屆 全國技能競賽 資訊與網路技術 Day1

競賽說明

- 本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求。
- 如在比賽過程中有任何疑問，或題意描述不清楚，請立即向裁判反應。
- 工作項目中須設定密碼之處，若試題未明確指定，則一律使用 Skills39
- 評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分。
- 除了必須以檢視設定值的方式進行評分的項目外，所有面向用戶的服務一律由用戶端系統進行功能測試，否則該項目不予計分
- 試題中 cXX、XX 等敘述，請選手代入自己的崗位號碼
- 選手將會取得專屬的 WAN_IP、DMZ_IP1、DMZ_IP2 共三組 Public IP，請在檢閱本試題時自行代入

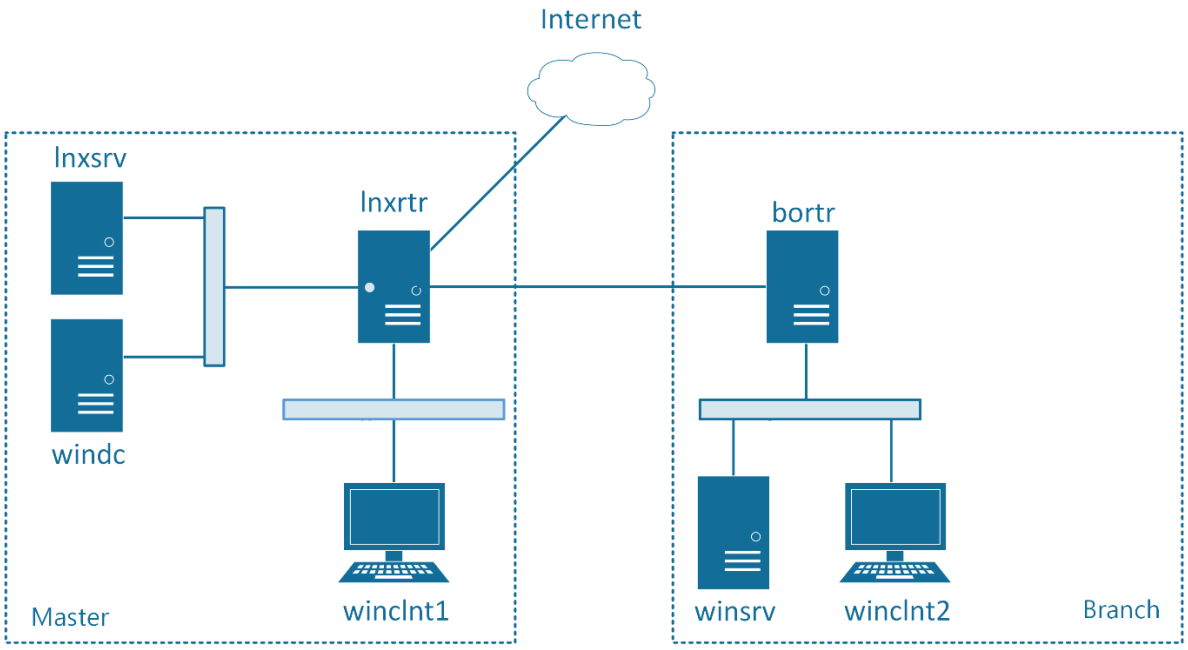
附錄 A、主機、網路相關設定

Hostname (.DomainName)	OS	Interface	IP Address	Default Gateway
lnxrtr	Debian 10	WAN	WAN_IP	100.100.100.129
		DMZ	150.150.150.1/24	
		LAN	192.168.1.1/25	
		Branch	10.1.1.1/30	
bortr	Debian 10	Master	10.1.1.2/30	
		LAN	192.168.1.129/26	
lnxsrv (.cXX.wsc.tw)	Debian 10	eth0	DMZ_IP1	150.150.150.1
windc (.ad.cXX.wsc.tw)	Windows Server 2019	Ethernet0	DMZ_IP2	150.150.150.1
winsrv (.ad.cXX.wsc.tw)	Windows Server 2019	Ethernet0	192.168.1.130/26	192.168.1.129
winclnt1-2 (.ad.cXX.wsc.tw)	Windows 10	Ethernet0	Via DHCP	

附錄 B、Active Directory 使用者與群組

Username	Group	Password
IT01-IT50	IT	Skills39
Sales01-Sales90	Sales	
Mkt01 – Mkt40	Marketing	

Network Diagram



Infrastructure Deployment

- 利用提供的 ova 檔部署公司內部的作業系統並依附表設定主機名稱及網路
- 將 lnxrtr 與 bortr 組態為路由器，使 Master 與 Branch 能夠相互存取
- 於 lnxrtr 設定 NAT，並使所有主機均可存取 Internet
- 於 lnxrtr 與 bortr 建立 IPsec，加密所有在此線路上傳輸的流量，Pre-shared Key 為 Skills39

Active Directory

- 於 windc 建立 ADDS，網域名稱為 ad.cXX.wsc.tw，並依附表新增使用者及群組

DHCP

- 於 lnxsrv 提供 DHCP 服務，配發 Master、Branch 的 Client 網段 IP，以 windc 為 DNS 伺服器
- 於 winsrv 設定 DHCP Relay Agent，讓 Branch 得以取得 lnxsrv 配發的 IP 位址

DNS

- 於 lnxsrv 提供 DNS 服務，管理 cXX.wsc.tw 網域，並依試題需求配置適當的記錄
- 域名 cXX.wsc.tw 已向供應商購得，請於 http://nsc.wsc.tw 進行授權資訊的配置
- 為增進安全性，當 lnxsrv 上的 DNS 服務接收到 Version Query 時，

  將回應 DNS Response Code 5 (REFUSED)
- 於 windc 提供 DNS 服務，管理 ad.cXX.wsc.tw 網域，並依試題需求配置適當的記錄
- 於 lnxsrv 將 ad.cXX.wsc.tw 子網域授權至 windc 管理，至此，本次競賽所有 DNS 記錄

  應可由來自網際網路的用戶、透過公眾 DNS 伺服器查詢並解析

CA

- 將 winsrv 組態為 Certification Authority，並依需要核發憑證

Active Directory

- 將 winclnt1 與 winclnt2 加入網域，並於兩部主機的 ad\Administrator 帳戶，

  提供 32 位元(i386)的 dig 與 vim 指令，可經由 debian run dig/vim 等方式使用
- 僅允許使用 TLS 或帶有完整性驗證的 Bind Request，存取 LDAP 服務
- 停用 Edge 第一次啟動時的初始設定頁面，並將首頁設定為 http://nsc.wsc.tw

Web

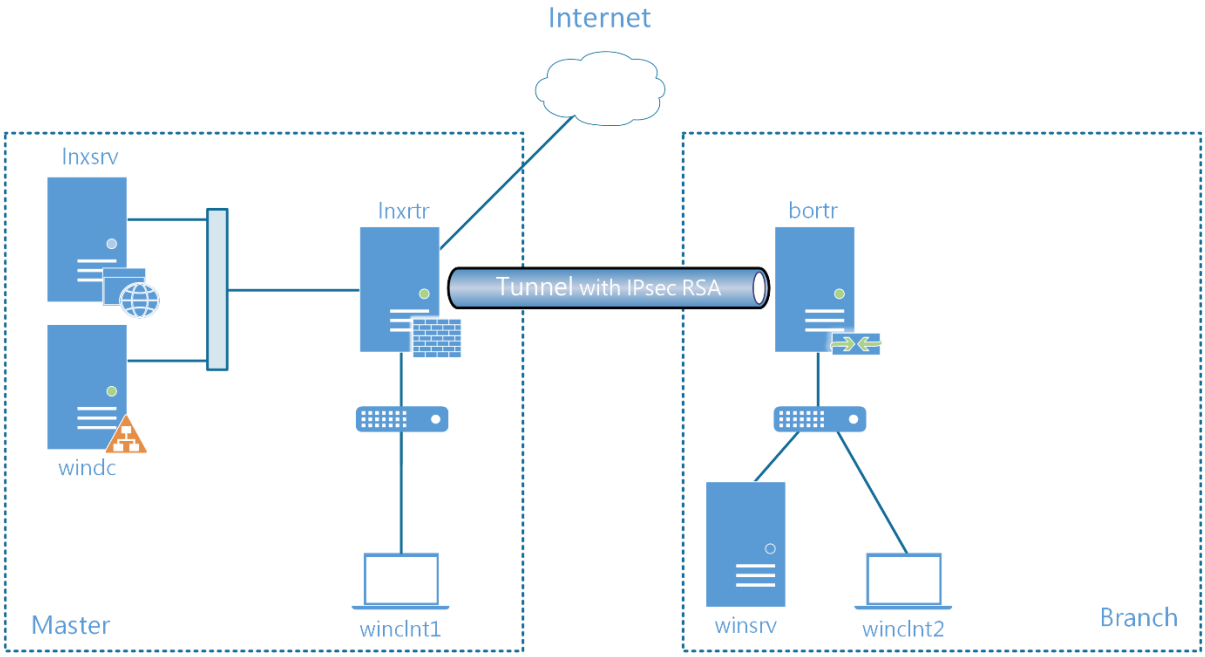
- 於 lnxsrv 提供 www.cxx.wsc.tw 站台，建立簡單的頁面以利測試，僅提供 HTTPS，若以 HTTP 存取時，將回應 TCP RESET
- 每 5 分鐘於 winsrv 發出測試請求，監控 lnxsrv 上的 Web 服務，並將 Response Header 記錄至 C:\www_check_result.txt
- 若 Web 請求來自 winsrv，則不在 lnxsrv 上生成 Access Log

Share Folder

- 於 winsrv 提供 \\file.ad.cxx.wsc.tw\public 分享資料夾，僅允許以 SMBv3 存取，
  網域使用者登入後，將自動掛載至磁碟機 P

第五十一屆 全國技能競賽 資訊與網路技術 Day2

Network Diagram



- 今日工作項目將延續昨日之情境，部分資訊請選手自行參考前一日的試題

Web

- 將 www.cXX.wsc.tw 站點的憑證改為使用 Let's Encrypt 簽發
- 提供 https://access.cXX.wsc.tw，並使用 Active Directory 的 LDAP 服務進行使用者驗證，僅允許 Sales 群組的使用者能夠存取

DNS

- 於 windc 管理 192.168.1.0/24 網段的反解紀錄，供內部資訊系統使用，並將 192.168.1.1 對應至 lnxrtr.cXX.wsc.tw
- 於 winsrv 提供 DNS 服務，管理 192.168.1.128/26 網段的反解紀錄，並將 192.168.1.129 對應至 bortr.cXX.wsc.tw
- 於 windc 進行子網域授權，將 192.168.1.128/26 的反解查詢委派至 winsrv 進行解析

Share Folder

- 為分享資料夾\\file.ad.cxx.wsc.tw\public 設定空間節省機制，分析多個檔案中相同的資料片段，並進行映射與清理，節省磁碟空間的佔用
  (Hint: Windows 10 與 Windows Server 的.iso 檔，內部資料的同質性相當高，可用於驗證該機制的運作效果)

Network Security

- 將 lnxrtr 與 bortr 之間的 IPsec 改為使用憑證驗證

Access Control - lnxrtr

- 由外部 Internet 所發起的請求，僅能存取公司的 DNS 與 Web 服務，其餘一律阻擋並紀錄至 /var/log/firewall/deny.log，其中格式為 "<date> <src-ip> <dst-port>"
- windc 對內不做任何網路限制，lnxsrv 僅允許向 Internet 送出 ICMP Echo Request
- 同一來源 IP 每小時不應該對 bortr 的 WAN 介面送出超過 200 個 ICMP Ping，請針對此類封包，將來源 IP 及其目前的狀態(是否超額)記錄至 /var/log/firewall/icmp_limit.log，記錄格式同樣應包含時間戳記

DNS

- 將公司內部所有 DNS 伺服器組態為 DNSSEC Resolver
- 為 cXX.wsc.tw 與 ad.cXX.wsc.tw 的正解區域導入 DNSSEC

Automation

- 請參考所提供的 DNS API 指引，並在 lnxsrv 上建立 Script，放置於/srv/script/中，自動化未來更新 DNSSEC Key 的步驟 (將 KSK 的 Digest 導出並更新上層供應商的相關紀錄