陸軍建置網路安全測試環境之研究

作者／曾鴻麟少校

提要

一、目前世界各先進國家都非常重視資訊科技並運用於作戰，中共早已成立網軍，國軍必須及早因應。

二、網路安全已是生活中不可忽視的問題，民間早已著手相關領域的研究，如何建置一個擁有專屬實驗設備與空間的實驗室，並提供學者專家進行相關的網路安全實驗，是必須事先克服的問題。

三、有良好的網路安全測試環境，提供人員訓練研究，方能使陸軍網路防護能力更上一層樓。

關鍵詞：網路安全測試環境、虛擬化技術、模擬。

前言

目前世界各先進國家都非常重視資訊科技並運用於作戰，中共早已成立網軍，除數量龐大的正規部隊外，甚至納入民間駭客等戰力，國軍必須及早因應。而陸軍為國軍中人數最多的軍種，如能提升整體素質，妥善運用資訊科技，必能於未來網路戰中有所幫助。

為使本軍對各種網路攻擊手法更加了解，並能透過人員訓練及實際操作提高網路防護能力，本研究先透過近年來的網路攻擊事件了解網路安全的重要性，並研究建置網路安全測試環境之技術，再從目前民間與陸軍現行作法中，探討建置網路安全測試環境之方式，最後提出結論與建議。

網路安全威脅

一、近期網路攻擊案例

(一)美國Target公司個資外洩(2014年)

1.事發經過

駭客竊取美國第二大美國零售百貨集團(Target)公司空調系統服務廠商設置的帳號密碼，以網路管理者登入取得最高權限帳號，進而入侵其企業網路，盜取用戶信用卡資訊，導致數千萬筆資料於黑市流通。

2.影響

(1)顧客個資外洩高達 7000 萬筆。

(2)4000 萬筆信用卡資料於黑市流通。

(3)損失超過 10 億美金，並賠償消費者 1,900 萬美金。

(二)菲國政府DNS主機遭攻擊(2013年)

1.事發經過

因不滿菲律賓槍擊台灣漁民，國內網友發起「鍵盤戰爭」，而署名 Anonymous 的國際駭客組織更攻陷菲國政府 gov.ph 的 DNS 主機，取得許多菲國政府網站管理帳號、密碼，足以對菲國政府網站發動大規模攻擊。

2.影響

(1)首頁遭置換。

(2)2，300 個菲國政府網域 DNS 管理者的帳號、密碼遭公布[1]。

(三)法國TV5Monde遭攻擊事件(2015年)

1.事發經過

針對法國 TV5Monde 電視網的大規模網路攻擊，當時該電視網的 11 個頻道都被停播了，Facebook 網頁被用來發布據稱來自伊斯蘭國 ISIS 的宣傳資訊。Twitter 帳號也被用來貼出反對美國和法國的留言，以及發出威脅法國士兵家屬的訊息。

2.影響

(1)TV5Monde 所有頻道的播出完全中斷。

(2)TV5Monde 的內部網路完全中斷。

(3)取得 TV5Monde 網站和社群媒體帳號的控制。

(4)變更網站內容成為親 ISIS 的聲明。[2]

(四)南韓遭網路攻擊事件(2013年)

1.事發經過

北韓 8 個月的精心策劃和暗中執行，於 3 月 20 日對南韓發動攻擊，包括 6 間金融機構及 3 家電視台都受到影響暫停服務，受害者有新韓銀行、農協銀行、濟洲銀行、KBS、MBC 和 YTN 等，堪稱近年來規模最大的網路攻擊事件。

2.影響

(1)32,000 台電腦遭駭停擺。

(2)6 間金融機構及 3 家電視台都受到影響暫停服務。

(3)1 家電信公司因此關閉對外網路服務。

[1] http://www.ithome.com.tw/node/80289,2017/4/23.

[2] https://blog.trendmicro.com.tw/?p=12074,2017/4/23.

(4)7 天才能完全復原。[3]

(五)索尼影業遭攻擊事件(2014年)

1.事發經過

索尼影業駭客入侵事件是發生於 2014 年 11 月 24 日的一場攻擊事件。駭客組織「和平衛士」聲稱從索尼獲得超過 100TB 的資料，並公布索尼影業員工電郵，涉及公司高管薪酬和索尼非發行電影拷貝等內容，要求不得公開放映《名嘴出任務》電影。

2.影響

(1)索尼影業員工電郵遭公布。

(2)索尼影業內部硬碟遭損毀，公司停擺。[4]

(六)美國防機密遭駭(2013年)

1.事發經過

28 歲英國駭客勒夫，涉嫌與 2 名澳洲與 1 名瑞典共犯，自 2012 年 10 月到 2013 年 7 月，多次入侵美政府系統涉嫌駭進美軍、國防部、美國航太總署（NASA）電腦系統盜走大量足以搞垮美國的機密資料，造成數百萬美元損失。

2.影響

(1)大量機密資料遭竊。

(2)造成數百萬美元損失。[5]

(七) ATM盜領事件(2016年)

1.事發經過

駭客從第一銀行分行入侵內網，建立內網潛伏基地，並暗中蒐集入侵情報，開啟 ATM 遠端控制植入 ATM 控制木馬，發動盜領，累計盜走 8,327 萬 7,600 元。

2.影響

第一銀行臺北和臺中市合計有 22 家分行共 41 臺 ATM 都遭人清空，累計遭盜走了 8,327 萬 7,600 元。[6]

二、常見網路威脅與攻擊趨勢

(一)常見網路威脅

1.弱密碼

就是指容易破譯的密碼，多為順序或重複的字母、簡單的數字組合、常用的單字、詞、帳號相同的數字組合、鍵盤上的臨近鍵、常用數字或常見姓名等，不管系統

[3] http://www.ithome.com.tw/node/79740,2017/4/23.
[4] http://www.ithome.com.tw/news/93457,2017/4/23.
[5] http://www.appledaily.com.tw/appledaily/article/international/20131030/35401979,2017/4/23.
[6] http://www.ithome.com.tw/news/107294,2017/4/23.

防護如何嚴密，存在「弱密碼」漏洞就容易被破解[7]，圖一為 2016 年弱密碼統計。

圖一 2016 弱密碼統計

資料來源：https://morread.com/90XDXE.html, 2017/4/23.

2.分散式阻斷服務攻擊

是指攻擊者下達指令給控制主機，由控制主機去操控代理主機，利用這些代理主機於同一時間內發動攻擊來癱瘓目標的一種攻擊方式。[8]

3.漏洞攻擊

是指利用還沒有修補的安全漏洞進行的攻擊，對網路安全具有巨大威脅，對犯罪駭客而言，具有極高的利用價值，一些國家間諜和網軍部隊，也非常重視這些資訊[9]。

4.跨網站指令碼(Cross-site Scripting, XSS)攻擊

是一種利用網站應用程式安全漏洞進行的攻擊，攻擊者將程式碼注入到網頁上，其他使用者在觀看網頁時就會載入並執行攻擊者惡意製造的網頁程式[10]，攻擊流程如圖二。

5.網路釣魚

通常是透過 e-mail 或者即時通訊進行，導引用戶到網址及介面外觀與真正網站幾無二致的假冒網站，以獲得如帳戶、密碼和信用卡明細等個人敏感資訊，除造成損失外，可能成為有心人士後續攻擊的前奏。[11]

---

[7] http://www.twword.com/wiki/%E5%BC%B1%E5%AF%86%E7%A2%BC, 2017/4/23.
[8] http://2010.e98.org.tw/securitynews/index21.htm, 2017/4/23.
[9] https://zh.wikipedia.org/wiki/%E9%9B%B6%E6%97%A5%E6%94%BB%E5%87%BB, 2017/4/23.
[10] https://zh.wikipedia.org/wiki/%E8%B7%A8%E7%B6%B2%E7%AB%99%E6%8C%87%E4%BB%A4%E7%A2%BC, 2017/4/23.
[11] https://blog.trendmicro.com.tw/?p=136, 2017/4/23.

圖二 XSS 攻擊流程

資料來源：http://www.lijyyh.com/2013/06/web-application-security- risks-and.html, 2017/4/23.

6.進階持續性威脅(Advanced Persistent Threats, APT)

是一種針對特定政府或企業，長期間進行有計畫性、組織性竊取情資行為，取得受駭目標的控制權後，進行低調及緩慢的潛伏，並伺機存取整個目標網路竊取資料[12]。

7.網路巨砲

為中共利用對境外網站所設立的國家及防火牆，將中國境外的流量轉變為武器的一種網路攻擊方式，此種將綁架的流量轉移至特定的目標，其功效類似分散式阻斷服務攻擊，以大量的網路流量癱瘓目標[13]。

(二)攻擊趨勢

1.勒索軟體日漸猖獗

根據趨勢科技的數據顯示，近年來受到勒索軟體感染的個人及公司數量不斷向上攀升，攻擊手法也不斷變種[14]，甚至連蘋果電腦的作業系統也有被攻擊成功的案例，

[12] https://blog.trendmicro.com.tw/?p=123, 2017/4/23.
[13] https://www.inside.com.tw/2015/04/13/great-cannon-of-china, 2017/4/23.
[14] 行政院國家資通安全會報技術服務中心，〈攻擊趨勢與常見攻擊手法〉，http://download.nccst.nat.gov.tw/Fattachfilenew/議題1_攻擊趨勢與常見攻擊手法.pdf，2017年4月23日。

專家指出行動裝置及穿戴裝置也是攻擊的目標，雖然目前沒有成功的案例，但是已證實在技術上可行。可以看出未來勒索軟體的攻擊方式朝向多元化發展，讓人防不勝防，造成使用資訊產品時的困擾，也是各種廠商對產品資訊安全保護的嚴苛挑戰[15]。

2.物聯網助長傀儡大軍

趨勢科技資深協理張裕敏曾表示，越受歡迎且越多人愛用的新興科技，就是駭客努力鑽研的新領域[16]，而物聯網是目前的熱門資訊運用，各式各樣的物品及裝備能藉由網路互相連接，使生活更有智慧，相關的討論及應用方式隨處可見。但是這些藉由網路串聯的裝置中，大多缺乏資安防護，只要連上網路，就跟所有的資訊設備有著相同的威脅，不管是漏洞、非法存取及服務中斷等，甚至成為傀儡網路的一員，淪為駭客賺錢的工具，助長分散式阻斷服務攻擊[17]。

3. APT攻擊難以防範

近年來的駭客開始以各式網路攻擊手法淘金，不管是 DDoS 攻擊、變臉詐騙(Business Email Compromise, BEC)、商業流程入侵(Business Process Compromise, BPC)及零時差漏洞攻擊等，都造成企業損失慘重。因為此種地下經濟收益高，各種不同專業技術的駭客開始群聚並分工，降低 APT 攻擊的成本，使得此種持續性的攻擊在未來仍是公司企業的心頭大患。[18]

網路安全測試環境

一、網路安全測試環境簡介

由於網際網路的發展與普及，網路安全已是生活中不可忽視的問題。有鑑於此，民間早已著手相關領域的研究，其中有一個最大的問題就是研究環境的建置，如何建置一個擁有專屬實驗設備與空間的實驗室，並提供學者專家進行相關的網路安全實驗，是必須事先克服的。[19]

網路安全測試環境為一種具隔離性，可實施科學實驗，且不影響真實網路的實驗環境，建置後可以提供資訊相關研究人員實施網路攻擊、防禦及各種網路安全技術研究[20]。以國軍的性質來看，太多機敏性的問題存在，所以訂定了非常嚴格的資安規定，管控各式網路、硬體及軟體，在如此環境下資訊人員因受到各種限制，實在難以持續

[15] 林子煒，〈2017 年資安趨勢分析〉，http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=3762，2017 年 4 月 23 日。
[16] 同註 15。
[17] 趨勢科技全球技術支援與研發中心，〈趨勢科技 2017 資安預測公布：資安威脅三高 駭客淘金熱潮來襲！〉，https://blog.trendmicro.com.tw/?p=38779，2017 年 4 月 23 日。
[18] 同註 17。
[19] 賴溪松，〈台灣網路安全測試平台之建置〉，國立成功大學資通安全研發中心，民國 105 年 6 月 26 日，頁 1。
[20] 陳培德，〈網路安全測試平台簡介〉，http://tnrc.ncku.edu.tw/course/93/930401.pdf，2017 年 4 月 23 日。

練習精進，所以本軍建置網路安全測試環境確有其必要性。

二、實體環境建置

一個環境的建置，一般來說會想到是實際上的環境。實體的網路安全測試環境一定會需要網路、用戶及伺服器等，這就牽扯到網路設備、終端設備及設置的場地，且為了設備的妥善，存管的位置也不可隨便，溫度濕度都要控制好。

因為使用真實的設備，所以實驗數據都會跟實際網路環境測試時的結果一樣，非常好用，但是這種實體環境建置存在一些缺點，敘述如下：[21]

(一)操作者必須到現場，進行環境建置及各種設定。

(二)實驗進行中，若因任務中斷實驗，其他人可能也無法共享資源，造成資源浪費。

(三)實驗數據及資料均需額外收集保管，使用不便。

(四)如擴充實驗時，需花費大量時間調整設備及環境。

(五)實體設備價格昂貴。

三、虛擬化技術

在成本、使用成效及彈性的考量下，民間也有使用虛擬化技術建置網路安全實驗室，方式分別說明如下：

(一)模擬(Simulation)

以軟體模擬功能及運行結果，最後呈現出來，是一種運用數據計算模擬的環境，如 NS2(Network Simulator Version 2)[22]及 Cisco Packet Tracer 等，需要將模擬軟體安裝於電腦上，可以展現出一些簡單的實驗及結果。

(二)虛擬機器(Virtual Machine)

是將硬體資源隔離出來，讓作業系統認為自己擁有完整的電腦資源，可以在一台電腦上同時運作多個作業系統，而非是在一部電腦上安裝多個作業系統的多重開機。此種方式可以一機多用，將硬體中的資源充分利用，且效果如同實體電腦。

使用者可以在建立的虛擬機器上自由的操作作業系統及安裝各種軟體，也可進行攻擊行為或測試病毒，常用的虛擬機器有 VMware[23]及 Hyper- V[24]等。

四、建模與模擬技術[25]

運用的是建模與模擬方法(Modeling and Simulation Methodology)，可用來建立環境

---

[21] 同註 19。

[22] http://italics.ee.kuas.edu.tw/NS2.htm l,2010/5/13.

[23] http://www.vmware.com ,2010/5/13.

[24] http://www.microsoft.com/zh-tw/download/details.aspx=3702,2010/5/13.

[25] 翁興國，〈網路攻擊與防禦訓練系統之建模與模擬技術探討〉，國立臺灣大學資訊通信研究所，民國 103 年 4 月，頁 1。

進行網路攻擊與防護訓練，在網路攻擊與防禦訓練系統之建模與模擬技術探討此篇文章中，列出 5 種具代表性的系統，其中 ARENA 系統、MAADNET 網路、NADSTS 系統及 Network Defense Trainer 為軟體的系統，特色是能夠模擬部分網路攻擊及防護模型，Network Defense Trainer 的攻擊工具甚至真實到可能會被用來發動網路攻擊。而「網路安全測試評台(Testbed@TWISC)」則是運用真實網路設備、伺服器及軟體來建立網路模型，能展現出真實的效果。

我們透過比較表來分析各種建置方式的優缺點(如表一)，因建模與模擬技術大部分為模擬，故不另做比較，從表一中可以發現，各種方式皆有其優缺點。

表一 網路安全測試環境建置方式優缺點比較表

	實體環境建置	模擬	虛擬機器
優點	1.真實性高。 2.系統效能佳。 3.可進行大規模網路的模擬。	1.建置成本低。 2.操作使用方便。	1.建置成本低。 2.操作使用方便。 3.真實性高。
缺點	1.建置成本高。 2.實驗規模大時管理困難 3.變更實驗項目時操作不便	1.真實性低。 2.部分功能無法模擬。 3.必須安裝於電腦上。	1.效能不及真實設備。 2.佔用較大的硬體支援 3.只能進行小型網路的模擬

資料來源：作者整理。

現行作法與運用方式

一、民間現行作法

目前民間已在使用的方式很多，如成功大學資通安全研發中心接受電信國家型科技計畫的經費補助，建置的「網路安全測試平台」，以及利用虛擬化技術建置的虛擬化網路安全實習實驗室等[26]，以下分別介紹：

(一)臺灣網路安全測試平台

為國立成功大學資通安全研發中心建置的，是一種仿真(Emulation)的架構。從 2006 年 16 的網路節點開始，一直到 2010 年擴充至 198 個網路節點，花費了新臺幣至少 3 億 5 千萬元以上。可以讓使用者透過介面選擇要使用的網路設備及電腦，建構各種網路測試環境，這些網路設備及電腦是真實存在的，且可以多人共用，當一組實驗暫停時，如果另一組實驗需要用到設備，系統會調整，但是實驗的紀錄都會保存，提供第一組實驗繼續時使用。此平台至今已支援多個研究團隊與使用者實施研究與實驗，且每年舉辦大型推廣活動及全國資訊安全營，成效良好。[27]

[26] 梁德昭、陳俊廷，〈虛擬化網路安全實習實驗室之規劃與建置〉，淡江大學資訊管理研究所，民國 105 年 6 月 26 日，頁 1。
[27] 同註 20。

(二)虛擬化網路安全實習實驗室[28]

以虛擬化(Virtualization)技術為基礎，利用 Xen Linux 為作業系統核心，開發虛擬化的實驗環境，並以 OpenVZ 在 Xen 虛擬環境下建立提供實驗使用的作業平台，管理人員可設定實驗的還原及備份，靈活配置實驗設備，而使用者是以 VPN 的方式透過網路連線到作業平台，只要伺服器硬體效能足夠即可提供大量使用者使用。[29]

(三)雲端資安攻防平台[30]

為科技部委由國家高速網路與計算中心執行資訊安全開放資料平台研發與惡意程式知識庫維運計畫之一部分，此平台是以雲端服務及虛擬化的架構建立，具備「專屬隔離環境」及「擬真場域實戰」兩大特色，可提供快速部署攻防演練場景，同時進行多人多場景的攻防演練環境，讓參與的人員能從中學習資訊安全的檢測與分析技巧。自 2016 年「雲端資安攻防平台」上線測試以來，已至全國各大專院校進行試辦，共 50 所大專院校、60 個系所參與，同時也可作為攻防競賽舞台，訓練攻防實戰人才。[31]

二、國軍現行作法

既然民間早已有相關技術，國軍當然也有發展，分述如下[32]：

(一)資訊安全鑑識實驗室(通次室)

於民國96年建置，實驗室環境包含機房等軟硬體設備花費約新臺幣300萬元，可提供資訊戰入侵行為研析、資訊戰入侵誘捕技術與回溯追蹤技術研究等，目前由支援通次室資安處的資安區隊負責管理，主要任務以協助國軍資訊安全鑑識為主。

(二)資訊安全教育訓練中心(國防大學理工學院)

在民國95年建置，並於105年時更新軟硬體設備，為一實體架構之大型網路安全測試環境，負責國軍資訊戰人才之培育及資訊戰攻防相關研究案等，目前由理工學院資工系負責管理。105年開始在通次室指導下，運用此環境舉辦軍校盃網路安全競賽，藉由競賽方式促進交流，提升國軍網路安全素質。

(三)網路攻防訓練室(資通電軍指揮部)

又稱為網路攻防靶場，於民國102年建置，當時花費約400萬元，包含資訊機房、展示螢幕、冷氣及桌上型電腦等，是一混合式架構的網路安全測試環境，目前由網路戰聯隊管理，可提供資訊戰戰具戰場環境驗證、資訊戰相關新興作需研擬等。此訓練室除可進行網路攻防實驗，也作為網路攻防技術及專題研討的場所，為資通電軍培育

---

[28] 同註 26。
[29] 同註 26。
[30] https://cdx.nchc.org.tw/introduction.php, 2010/6/18.
[31] https://www.nchc.org.tw/tw/news/index.php?NEWS_ID=309, 2010/6/18.
[32] 李建中，〈中共網軍發展與對我威脅之分析〉《陸軍通資半年刊》，第 124 期，陸軍通信電子資訊訓練中心，民國 104 年 9 月。頁 4。

優秀人才。

雖然國軍已規劃以上相關實驗室，做為網路安全測試環境使用，但是陸軍卻無相關的環境，且對於本軍龐大的架構及繁重的業務來說，這種大規模且花費高的實驗室不一定合適。因此，可從民間的技術中研究適合本軍的網路安全測試環境，並推廣設置，讓資訊人員能透過訓練及實際操作提高整體網路防護能力，從基層開始建構本軍網路戰戰力。

三、網路安全測試環境運用方式

參考民間已在使用之方法、本軍任務及特性，除了考量價格外，建議在本軍建置網路安全測試環境應該具備的功能如下：[33]

(一)隔離性

進行網路安全相關實驗時，勢必會進行入侵、探測及攻擊等行為，也會運用各種惡意程式，如果沒有隔離，很有可能會造成網路上正在運行的伺服器或是用戶遭受波及，而國軍網路為特殊網路環境，是不容許有任何的差錯發生。

(二)可儲存性

本軍任務繁重，資訊人力也不足，在進行網路安全實驗的過程中，有很大的機會因其他任務而中斷實驗，時間可能從數小時、數天、數週甚至是數個月，這時就需要將實驗的環境儲存，以利任務結束回到實驗中時可以繼續。

需要儲存的另一個原因是關於實驗方式，實驗常常會有各種假設，或是以試誤法(Try and Error)的方式進行，能像玩遊戲般存檔後選擇不同的方式進行，將有助於實驗的發展。

(三)可控制性

資訊人員對於自己進行的實驗要有完全控制的權限，任何限制都會對實驗造成影響，例如是否有管理者權限、有無資訊安全規定限制及模擬軟體是否可模擬等因素。

(四)便利性

依照國軍的現況，任務、管制及規定從來沒有少過，本軍若要建立此環境，必定會再新增若干管制規定、管制辦法、執行作法，甚至環境負責人等，對於本以業務繁重之本軍資訊人員又是一項壓力，可想而知，經過一陣子後，當上級長官不再在意此事後，網路安全測試環境就會慢慢荒廢，最後結束。所以此環境的管理及使用必須相當的便利，不會增加太多瑣碎的任務。

(五)通用性

網路安全測試環境根據前述目的，要進行各種實驗及訓練，所以能支援的項目越

[33] 同註 19。

多，成本效益越高。

根據上述條件，比較各種建置方式的功能如表二。在隔離性的部分，每一種方式都能達到要求；而可儲存性為模擬及虛擬機器較佔優勢；可控制性的部分模擬及虛擬皆有其限制，無法完全如實體裝置一般；在便利性的方面，虛擬的方式就能簡單的管理使用，但是通用性上就各有優缺點了，如實體環境建置可視設備狀況實施實驗，可是無法像模擬一般使用不存在的設備，但模擬器又無法完整模擬實體設備，只有混合式的能夠結合各種方式的優點，適合各式實驗及訓練，且在價格方面不會讓各單位壓力太大。最終比較結果，混合式的環境建置方式略勝一籌，尤其在通用性的部分，讓資訊人員可以視實驗項目使用實體、模擬、虛擬機器或是混合式進行實驗。

表二 功能比較表

方式 / 功能	實體環境建置	模擬	虛擬機器	混合式
隔離性	※※※	※※※	※※※	※※※
可儲存性	※	※※※	※※※	※※
可控制性	※※※	※	※	※※
便利性	※	※※※	※※※	※※
通用性	※	※	※	※※※
價格	**昂貴**	**一般**	**一般**	**一般**
※：依照標示的符號數量表示功能完整度				

資料來源：作者整理。

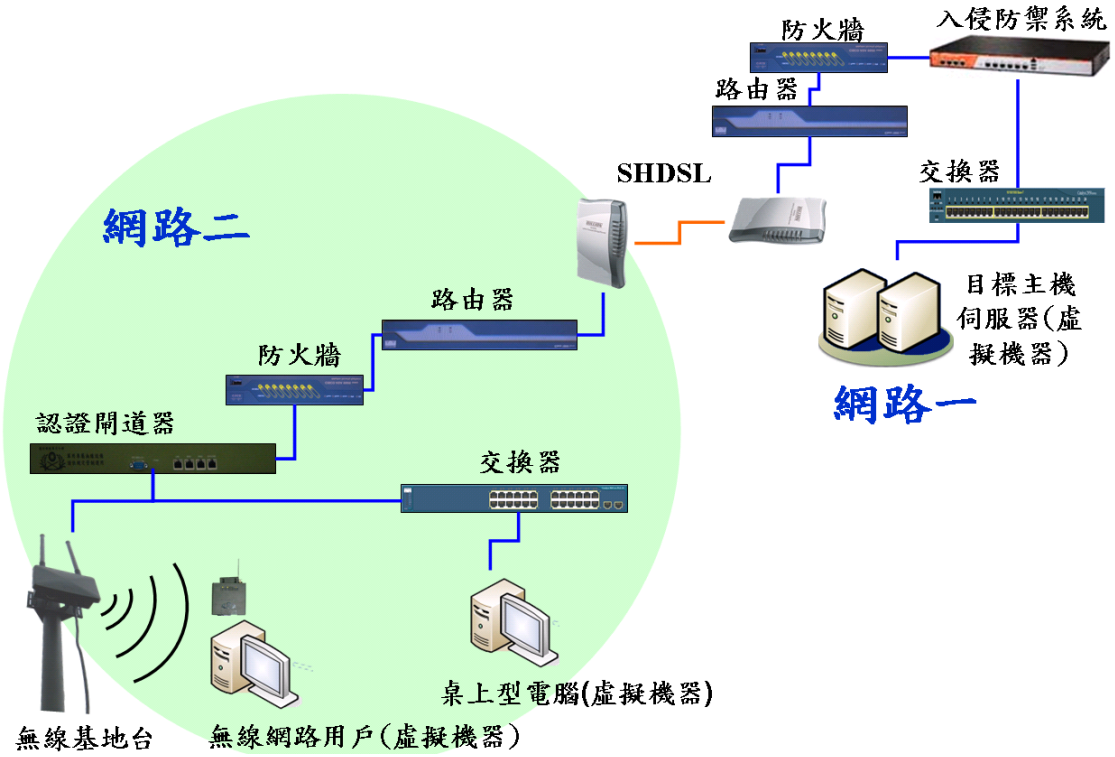
依前述運用方式及功能比較，以本軍的狀況來說，可以選用混合實體環境、模擬及虛擬機器的方式建置低成本、真實性高且操作方便的網路安全測試環境，規劃本軍網路安全測試環境如圖三，我們可以看到實體環境建置的部分，是運用現用的設備建置，為獨立網路，可包含網路及資安設備如交換器、路由器、防火牆及入侵防禦系統等，資訊人員使用時可隨意設定，提升熟練度。在虛擬機器的部分由數部電腦就可以模擬一定數量的電腦，可進行攻擊的模擬、防護的練習或是網路資訊收集等，也安裝基本的模擬軟體，提供人員訓練。另外，網路安全測試環境建置後，對於現行攻擊手法所能提供的研究及訓練架構，可依需求變更，如分散式阻斷服務攻擊、漏洞攻擊及跨網站指令碼攻擊等，未使用加密式無線網路及 SHDSL 設備，可調整移除，如下所述：

(一) 分散式阻斷服務攻擊

以目前電腦的效能來說，單純實施阻斷服務攻擊的效果已經不夠，所以現在的攻擊多是使用分散式阻斷服務攻擊，在規劃的網路安全測試環境中，我們可以在隔離的

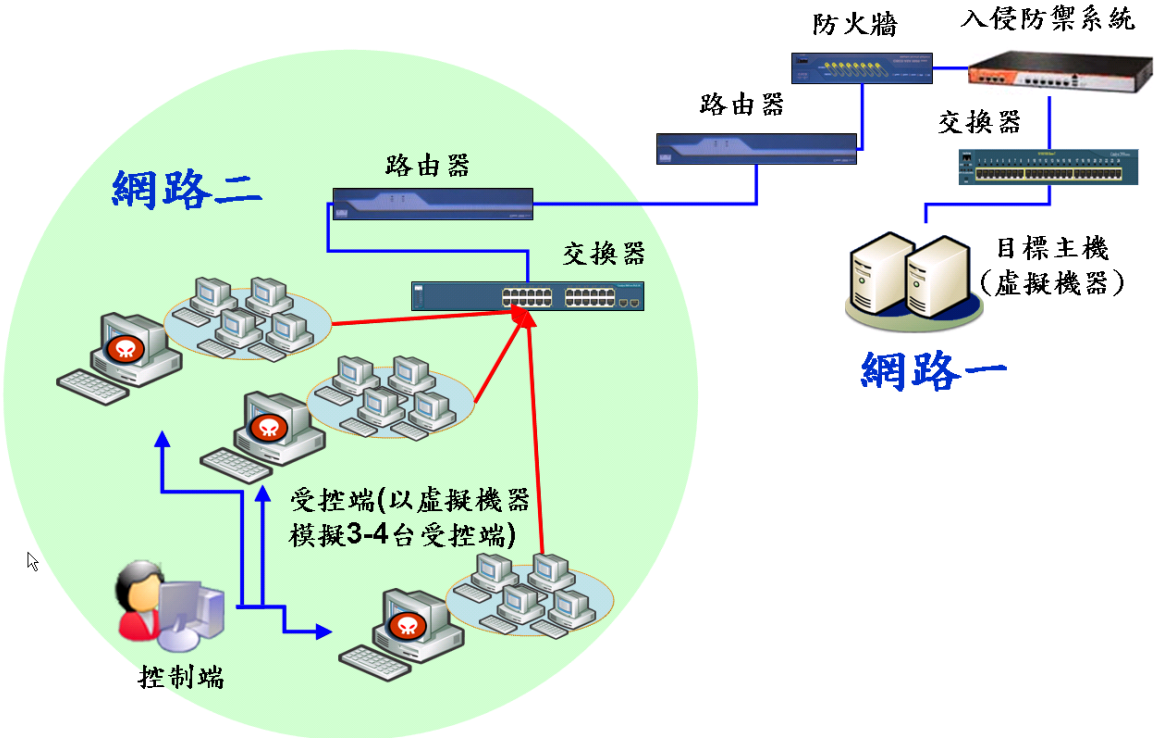
網路上，以數台電腦搭配虛擬機器軟體擔任控制端及受控端，模擬分散式阻斷服務攻擊，並於防護端模擬測試遭攻擊的狀況，之後可分別以個人防火牆、網路防火牆及入侵防禦系統等實施防護，並研究各種防護方式效能，架構如圖四。

圖三 網路安全測試環境建置示意圖



資料來源：作者繪製。

圖四 分散式阻斷服務攻擊架構示意圖

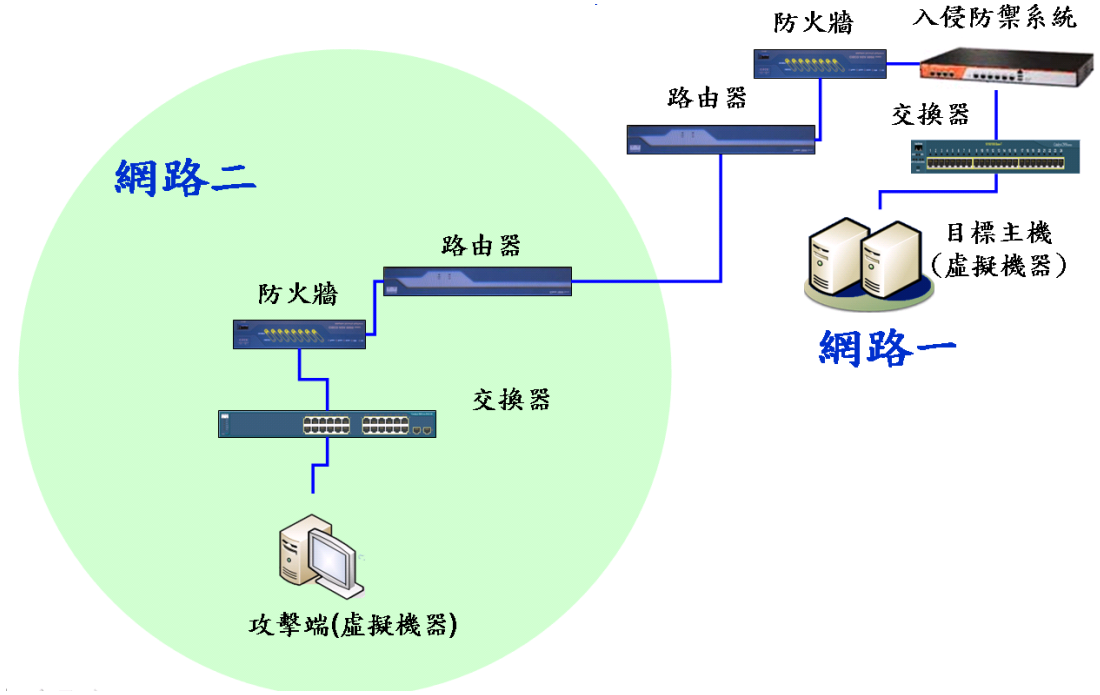


資料來源：作者繪製。

(二) 漏洞攻擊

漏洞攻擊是駭客喜歡的攻擊方式之一，只要執行了有漏洞的程式，就像在電腦上開了一扇門一樣，非常危險。所以，我們會看到微軟的作業系統，以及一些知名的應用程式不斷的在更新，而我們國軍也針對這些漏洞不時的發布資安通報。針對這些漏洞，陸軍也可以此環境測試，測試項目包含修補漏洞後的狀況，以及未修補漏洞時，防護系統能否保護設備等，且只需變動少部分裝備，架構如圖五。

圖五 漏洞攻擊測試環境示意圖



資料來源：作者繪製。

(三) 跨網站指令碼攻擊

此種攻擊方式是在網頁中放入惡意程式，而觀看的使用者會遭受攻擊，在本環境中架構其實無太大變化，可以虛擬機器模擬伺服器、攻擊端及受害用戶測試跨網站指令碼攻擊、修補網頁程式後之效果及用戶端的資安防護等進行測試，架構如圖六。

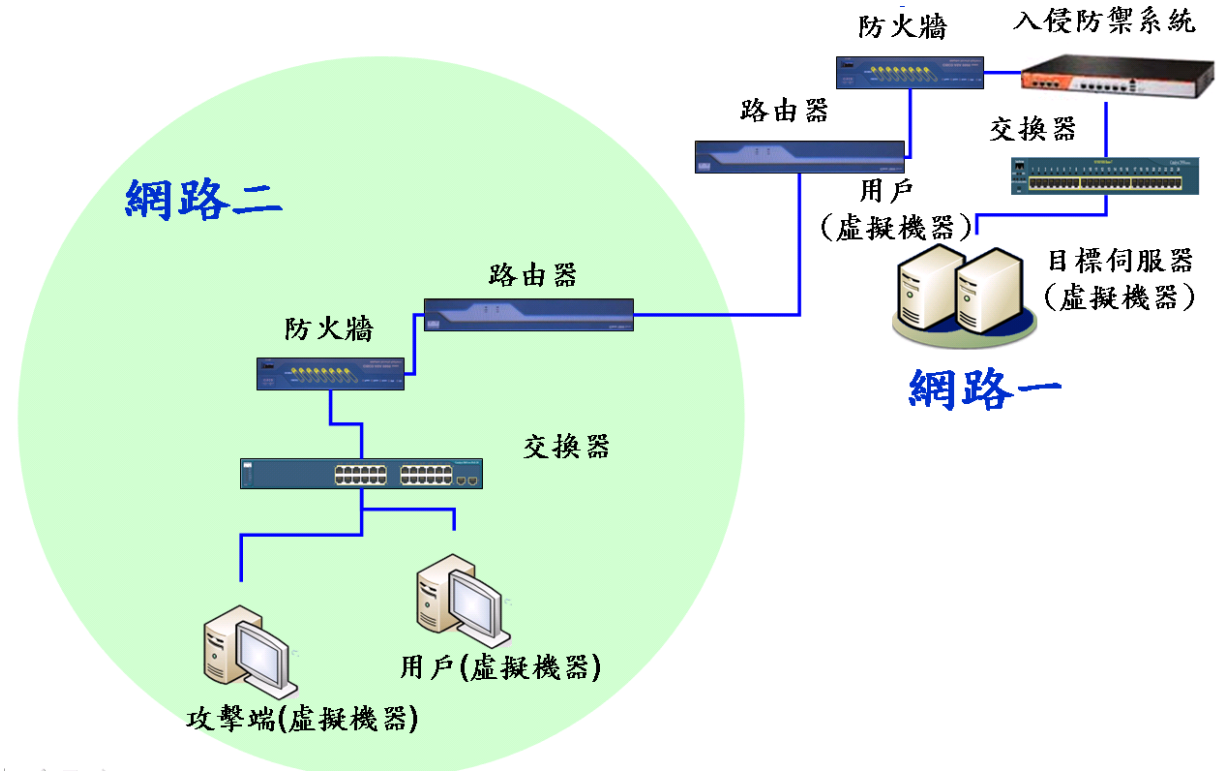
其餘如網路釣魚、進階持續性威脅、勒索軟體，以及一些網路設備的資安測試也可以運用本測試環境實施，要領如同前述架構，在文中不多做贅述。

結論與建議

身處網路科技發展迅速的時代中，來自網路上的威脅與日俱增，世界各國都密切注意著，尤其是我國面對世界強國中共的威脅，在網路戰上更是有著相當的戰力差距，國軍不能等閒視之，除了落實各項資訊安全政策外，對新的威脅與攻擊方式也必須了解與找尋因應之道，想要走捷徑投機取巧的打贏網路戰爭是一種不切實際的想法，最

好的方式就是透過提升人員的素質來強化網路戰的戰力。因此，須有良好的網路安全測試環境，提供人員訓練研究，方能使陸軍網路防護能力更上一層樓。

圖六 跨網站指令碼攻擊測試環境示意圖



資料來源：作者繪製。

本研究分析了建置網路安全測試環境的各種方式，按照本軍的各種任務及限制，發現混合使用各種環境建置方式是最適合的，理由說明如下：

(一) 建置成本低

規劃以現有未使用的裝備來建置小規模網路安全測試環境，不需編列預算或是協調上級經費來建置，降低資訊人員負擔。

(二) 環境真實且符合現況

使用現用設備建置環境，可使本軍資訊人員在測試環境中操作各種在本軍網路上無法安心測試之功能，更加熟練現用設備之操作。

(三) 靈活度大

混合式的環境建置依照前述的運用方式，只需小幅度修改即可實施各種小規模實驗，或利用模擬器熟練裝備。

根據以上分析，在本軍網路諸多限制的情況下，資訊人員確實需要一個網路安全測試環境來提升資訊人員的專業能力。且各單位建置文中介紹的混合型環境並不困難，建議本軍各單位可依據需求建置，期望能在推廣建置後，使本軍資訊人員擁有合適的訓練環境，透過扎實的訓練，提升本軍網路戰防護能力。

參考文獻

一、梁德昭、陳俊廷，〈虛擬化網路安全實習實驗室之規劃與建置〉，淡江大學資訊管理研究所，民國 105 年 6 月 26 日。

二、李建中，〈中共網軍發展與對我威脅之分析〉《陸軍通資半年刊》，第 124 期，陸軍通信電子資訊訓練中心，民國 104 年 9 月。

三、翁興國，〈網路攻擊與防禦訓練系統之建模與模擬技術探討〉，國立臺灣大學資訊通信研究所，民國 103 年 4 月。

四、賴溪松，〈台灣網路安全測試平台之建置〉，國立成功大學資通安全研發中心，民國 105 年 6 月 26 日。

五、行政院國家資通安全會報技術服務中心，〈攻擊趨勢與常見攻擊手法〉，http://download.nccst.nat.gov.tw/Fattachfilenew/議題 1_攻擊趨勢與常見攻擊手法.pdf，2017 年 4 月 23 日。

六、林子煒，〈2017 年資安趨勢分析〉，http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=3762，2017 年 4 月 23 日。

七、趨勢科技全球技術支援與研發中心，〈趨勢科技 2017 資安預測公布：資安威脅三高 駭客淘金熱潮來襲！〉，https://blog.trendmicro.com.tw/?p=38779，2017 年 4 月 23 日。

八、陳培德，〈網路安全測試平台簡介〉，http://tnrc.ncku.edu.tw/course/93/930401.pdf，2017 年 4 月 23 日。

作者簡介

曾鴻麟少校，中正理工學院專 89 年班、陸軍通信電子資訊學校通資安全正規班 10 期、國防大學理工學院資訊科學研究所 100 年班，曾任排長、副連長、教官，現任陸軍通信電子資訊訓練中心網作組教官。