建置資安攻防演練平台 從原理到實作

游子興 台大計中網路組 davisyou@ntu.edu.tw 02-33665008







- * 資安攻防平台架構
 - * 攻擊: Kali, OpenVAS
 - * 防守: Pfsense, Snort
 - * 受害: Metasploitable2, Win7(最初版) + Firefox, Win7(更新版)
- * 弱點偵察 Scan
 - * Nmap
 - * OpenVAS
 - Metasploit
- * 攻擊方式
 - * Direct Attack 直接攻擊
 - * Client Side Attack 用戶端攻擊
 - * Privilege Escalation 權限提升
- * 防守工具
 - * 防火牆: pfsense
 - * IPS:以 Snort 為例





資安攻防平台



National Taiwan Universit

VM 資源

VM	記憶體
Pfsense 2.4.4	512MB
Kali 2019.04	1GB
Metasploitable2	1GB
Win7 最初版	1GB
OpenVAS 6.00 (Option)	2GB

* VM 開啟時

* I Moved It: 不會變更 uuid & mac address * I Copied It: 會變更 uuid & mac address





資安攻防平台 Vmware 網路設定

Mode	VMnet	網卡	IP	DHCP	Internet
Bridge	VMneto	目前上網 網卡	Layer2	N/A	N/A
Host-only	VMnetı	VMware Network Adapter VMnetı	192.168.x.1	Yes	No
NAT	VMnet8	VMware Network Adapter VMnet8	192.168.x.1	Yes	Yes
	VMnetX	N/A	N/A	No	No

資安攻防平台 Pfsense 網路設定

Vi F	rtual Machine Settings DISENS lardware Options	е	
	Device	Summary	A
	📰 Memory	512 MB	
	Processors	2	
	⊟ Hard Disk (SCSI)	20 GB	
	💿 CD/DVD (IDE)	Auto detect	
	🔁 Network Adapter	NAT	WAN
	🔁 Network Adapter 2	Host-only	LAN_1
	Potwork Adapter 3	Custom (VMnet2)	LAN_2
	🕣 USB Controller	Present	
	📣 Sound Card	Auto detect	
	Display	Auto detect	





Pfsense 網路設定

Kali OpenVAS

Virtual Machine Settings

Η	lardware	Options		
	Device		Summary	
	📰 Mema	ory	1 GB	
	💭 Proce	essors	4	
	⊟ Hard	Disk (SCSI)	80 GB	
	💿 CD/D	VD (IDE)	Auto detect	
	🔁 Netw	ork Adapter	Host-only	LAN 1
	🕂 USB (Controller	Present	
	d) Soun	d Card	Auto detect	
	Displa	зу	Auto detect	

Metasploitable2 Win7 最初版

Virtual Machine Settings Hardware Options Device Summary E Memory 512 MB Processors 1 Hard Disk (SCSI) 8 GB 💽 CD/DVD (IDE) Auto detect 🔁 Network Adapter Custom (VMnet2) LA 🔄 Network Adapter 2 Host-only 🔄 USB Controller Present 🛄 Display . Auto detect



本機 Host 連線 LAN_1 設定

VMware Network Adapter ● 公 ● 公用 ● 公用 ● 認知能 ● 認知能 ● 認知能 ● 認知能 ● 認知 ● 認知能 ● 認知 ●		網際網路通訊協定第4版 (TCP/IPv4) - 内容	
VINITEL 如果您的網路支援道項功能,您可以取得自動指派的 IP 設定。否則,您必須 詢問網路系統管理員正確的 IP 設定。 VMware Network Adapter VMnet1 内容 自動取得 IP 位址(O) 確認方式: ● 自動取得 IP 位址(C) 運 VMware Vitual Ethernet Adapter for VMnet1 ② 意宜生命 ② 遵理錄使用下列項目(O): ③ ② ○ Eleand Printer Sharing for Microsoft Networks ③ ● Microsoft Networks ③ ● Microsoft Networks ③ ● Microsoft Networks ④ ● Microsoft Networks ④ ● Microsoft Networks ④ ● Microsoft Network Adapter 多工 器通訊協定 ④ ● Microsoft Networks ● ● Microsoft Networks ● ● Microsoft Networks ● ● Microsoft Networks ● ● Microsoft Network Adapter 多工 器通訊協定 ○ ● Microsoft Networks ● ● Microsoft Networks ● ● Microsoft Networks ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● <th>VMware Network Adapter</th> <th>一般</th> <th></th>	VMware Network Adapter	一般	
Wwwere Network Adapter VMnet1 内容 確認功能 使用 連線方式: ● 自動取得 IP 位址(0) 「 位址(0) ● 使用下列的 IP 位址(2): 「 P 位址(0): 192.168.92.1 ご Glient for Microsoft Networks ● 自動取得 IP 位址(2): 「 Client for Microsoft Networks ● 自動取得 IP 位址(2): 「 Client for Microsoft Networks ● 自動取得 DNS 伺服器位址(6) ● 使用下列的 IP 公址(2): ● 自動取得 DNS 伺服器位址(2): 「 目動取得 DNS 伺服器位址(2): ● 信用 T列的 DNS 伺服器位址(2): ● 使用下列的 DNS 伺服器位址(2): ● 信用 T列的 DNS 伺服器位址(2): ● 強服領路透明協定第 4 版 (TCP/IPv4) ● 自動取得 DNS 伺服器(2): ● 細胞得 Witrosoft LLDP 通訊協定驅動程式 ● 自動取得 DNS 伺服器(2): ● 細胞環網路透明協定第 6 版 (TCP/IPv6) ● 自動取得 DNS 伺服器(A): ● 試解時確認設定(L) ● 建 L ● 熔 和時確認設定(L) ● L 位 L(R) IP 位址 (R) ● P 位 址 (2) ● P 位 址 (2) ● 255.255.255.0 ● 192.168.92.1 255.255.255.0 ● 192.168.92.1 255.255.255.0 ● 192.168.92.1 255.255.255.0 ● 192.1100 ● 255.255.255.0	で Winell 記 記 思 用	如果您的網路支援這項功能,您可以取得 詢問網路系統管理員正確的 IP 設定。	寻自動指派的 IP 設定。否則,您必須
 ● 自動取得 IP 位址(0) ●使用下列的 IP 位址(1): 192.168.92.1 子網路速罩(U): 255.255.0 預設開道(D): ① 自動取得 IP 位址(1): 192.168.92.1 255.255.0 ●使用下列的 DNS 伺服器位址(B) ●使用下列的 DNS 伺服器位址(B) ●使用下列的 DNS 伺服器位址(E): ●使用下列的 DNS 伺服器(A): ○ ● 位址(R) □ 白動取得 DNS 伺服器(A): ○ ○<	VMware Network Adapter VMnet1 内容		
連線方式: ● 使用下列的 IP 位址(S): 「 位址(I): 192.168.92.1 一 255.255.0 通線線使用下列項目(O): ● 使用下列的 IP 位址(S): 「 位址(I): 192.168.92.1 空 Client for Microsoft Networks ● 「 VMware Bridge Protocol ● 「 VMware Bridge Protocol ● 「 YMM ware Bridge Protocol ● ● ● ● 和原網路通話服定 筆 4 版 (TCP/IPv4) ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	周路功能 驗證 共田	○ 自動取得 IP 位址(O)	
連線方式: IP 位址(0): 192.168.92.1 受定(C) 設定(C) 255.255.255.0 適個連線使用下列項目(O): 通設開道(D): 「Client for Microsoft Networks 自動取得 DNS 伺服器位址(B) ● 使用下列的 DNS 伺服器位址(E): 「用意用確認設定体」 ● 規範網路通訊協定第4.版 (TCP/IPv4) ● Microsoft Network Adapter 多工器通訊協定 文號(N) 解除安號(U) 內容(R) IP 位址 (R) IP 位址 子網路遊室 192.168.92.1 255.255.0 172.30.1.100 255.255.0		● 使用下列的 IP 位址(S):	
	連線方式:	IP 位址(l):	192.168.92.1
設定(C) 預設開道(D): 這個連線使用下列項目(O): ● 自動取得 DNS 伺服器位址(B) ● 注意 and Printer Sharing for Microsoft Networks ● 使用下列的 DNS 伺服器位址(E): ● 使用下列的 DNS 伺服器(P): ● 細際網路通訊協定第 4 版 (TCP/IPv4) ● Microsoft Network Adapter 多工器通訊協定 ● 使用下列的 DNS 伺服器(A): ● 使用下列的 DNS 伺服器(A): ● 使用下列的 DNS 伺服器(P): ● 補除空裝(U) 内容(R) □ 指束時確認設定(L) 進階(V) □P 位址 子網路遮置 192.168.92.1 255.255.0 172.30.1.100 255.255.255.0	VMware Virtual Ethernet Adapter for VMnet1	子網路遮罩(U):	255 . 255 . 255 . 0
✓ Client for Microsoft Networks ● 自動取得 DNS 伺服器位址(B) ✓ VMware Bridge Protocol ● 使用下列的 DNS 伺服器位址(E): ✓ File and Printer Sharing for Microsoft Networks ● 使用下列的 DNS 伺服器位址(E): ✓ 網際網路通訊協定第4版(TCP/IPv4) ● 使用下列的 DNS 伺服器(A): ▲ Microsoft Network Adapter 多工器通訊協定 ● 使用下列的 DNS 伺服器(A): ✓ Microsoft LLDP 通訊協定驅動程式 ● 位加 ✓ 網際網路通訊協定第6版(TCP/IPv6) ● 當束時確認設定(L) ④ 控催(R) □ 指束時確認設定(L) □ P 位址(R) □ P 位址(R) □ P 位址 子網路遮罩 □ 92.168.92.1 255.255.255.0 □ 172.30.1.100 255.255.255.0	設定(C) 這個連線使用下列項目(∩):	預設閘道(D):	· · ·
● 使用下列的 DNS 伺服器位址(E): ● 使用下列的 DNS 伺服器位址(E): ● 使用下列的 DNS 伺服器(P): ● 使用下列的 DNS 伺服器(P): ● 使用下列的 DNS 伺服器(P): ● 使用下列的 DNS 伺服器(A): ● Microsoft LLDP 通訊協定驅動程式 ● Microsoft LLDP 通訊協定	Client for Microsoft Networks	▲ 自動取得 DNS 伺服器位址(B)	
☑ File and Printer Sharing for Microsoft Networks ☑ 網際網路通訊協定第4版 (TCP/IPv4) ☑ Microsoft Network Adapter 多工器通訊協定 ☑ Microsoft LLDP 通訊協定驅動程式 ☑ 網際網路通訊協定第6版 (TCP/IPv6) ☑ 網際網路通訊協定第6版 (TCP/IPv6) ☑ 網際網路通訊協定第6版 (TCP/IPv6) ☑ 編除安裝(U) 內容(R) 内容(R) IP 位址 (R) 255.255.255.0 192.168.92.1 255.255.255.0 172.301.100 255.255.255.0	🗆 🕎 V Mware Bridge Protocol	● 使用下列的 DNS 伺服器位址(E):	
 Microsoft Network Adapter 多工器通訊協定 Microsoft LLDP 通訊協定驅動程式 網際網路通訊協定第 6 版 (TCP/IPv6) 新解除安裝(U) 内容(R) IP 位址(R) IP 位址(R) IP 位址 子網路遮罩 192.168.92.1 255.255.05 172.30.1.100 255.255.255.0 	✓ 號 File and Printer Sharing for Microsoft Networks ✓ ▲ 網際網路通訊協定第4版 (TCP/IPv4)	慣用 DNS 伺服器(P):	
 ✓ 網際網路通訊協定第6版(TCP/IPv6) ✓ Y ✓ Y<!--</td--><td> □ ▲ Microsoft Network Adapter 多工器通訊協定 ☑ ▲ Microsoft LLDP 通訊協定驅動程式 </td><td>其他 DNS 伺服器(A):</td><td></td>	 □ ▲ Microsoft Network Adapter 多工器通訊協定 ☑ ▲ Microsoft LLDP 通訊協定驅動程式 	其他 DNS 伺服器(A):	
安装(N) 解除安装(U) 内容(R) IP 位址 子網路遮罩 192.168.92.1 255.255.0 172.30.1.100 255.255.0	 ✓ ▲ 網際網路通訊協定第6版 (TCP/IPv6) ✓ ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	✓ 益東時確認設定(L)	進階(\/)
IP 位址 子網路遮罩 192.168.92.1 255.255.0 172.30.1.100 255.255.0	安装(N) 解除安装(U) 内容(R)	IP 位址(R)	
192.168.92.1 255.255.0 172.30.1.100 255.255.255.0		┛ IP 位址	子網路遮罩
172.30.1.100 255.255.255.0		192.168.92.1	255.255.255.0
		172.30.1.100	255.255.255.0

攻擊 - Kali

* SSH

- * Login: root
- * Passwd: toor
- * VMWare VM
 - * https://www.offensive-security.com/kali-linuxvm-vmware-virtualbox-image-download/
- * 工具
 - * Nmap
 - * Metasploit
 - * Netcat







Metasploit

- *初始化
 - * systemctl start postgresql
 - * systemctl enable postgresql
 - msfdb init
- * 開啟
 - msfconsole -q



Meterpreter Shell

- * 常用語法
 - getuid
 - sysinfo
 - * keyscan_start 鍵盤側錄開始
 - * keyscan_stop 鍵盤側錄結束
 - * screenshot
 - * 若出現錯誤:
 - * [-] stdapi_ui_desktop_screenshot: Operation failed: Access is denied.
 - * 原因:
 - * Windows 目前正使用 RDP 連線. 僅支援 Console 登入之下擷 取螢幕.





OpenVAS

* OpenVAS

- * http://172.30.1.3/
- * Login: admin
- * Passwd: admin_openvas
- * Virtual Appliance Version: 6.0.0
 - * https://www.greenbone.net/en/install_use_gce







Metasploitable

Metasploitable2

- * SSH
 - * Login: msfadmin
 - * Passwd: msfadmin
- * https://sourceforge.net/projects/metasploitable/
- * https://metasploit.help.rapid7.com/docs/metasplo itable-2-exploitability-guide
- * Metasploitable3 參考用
 - * https://github.com/rapid7/metasploitable3
 - * https://metasploit.help.rapid7.com/docs/settingup-a-vulnerable-target





Windows 7

Win7

- * 最初版本無任何 Patch
 * Console Login

 * Administrator Group
 * Login: user
 * Passwd: user

 * Not in Administrator Group

 * Login: test
 - * Passwd: test
- Firefox v28





受害方 Windows 7

💭 Computer Management	Lomputer Management
File Action View Help	File Action View Help
 Computer Management (Local) System Tools Task Scheduler Event Viewer Shared Folders Shared Folders Local Users and Groups Users Groups Device Manager Storage Disk Management Services and Applications 	 Computer Management (Local) System Tools Task Scheduler Task Scheduler Event Viewer Shared Folders Shared Folders Local Users and Groups Users Groups Member Of Profile Member of: Storage Disk Management Services and Applications
Every Search or enter address About Mozilla Firefox Image: About Mozilla Firefox Image: About Mozilla Firefox	Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all. Sound interesting? Get involved!

Ν

弱點偵察 Scan

* nmap

- * nmap -Pn -A 172.30.2.100
- * 結果: nmap_Metaspliable2.TXT
- * nmap -Pn -sC -sV -p 445 172.30.2.101
 - * -Pn Treat all hosts as online (skip host discovery), 若目的 ip 無法回應 ping
 - * -A OS detection + script scanning
 - * -sV Service version scanning
 - * -sC Scan using default safe scripts must be run with -sV switch in order for the NSE scripts (--script default)
- * OpenVAS* Metasploit



防守

Firewall

* Pfsense v2.4.4 p3
* http://172.30.1.1/
* Login: admin
* Passwd: pfsense
* https://www.pfsense.org/





防守 – IDS/IPS Snort in pfsense * System > Package Manager * 安裝 snort package

snort security 3.2.9.10 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

Package Dependencies: Snort-2.9.15 Sarnyard2-1.13_1

穩定版本: 2.9.15.0 (2019/10/10)

* Services > Snort > Global Settings

- * Enable Snort VRT= Check
- * Snort Oinkmaster Code=
- Services > Snort > Update Rules
 * Update Rules



Snort in pfsense Install & Setup

* Services > Snort > Interfaces

- * Interface= LAN_2
- * Home Net= HomeNet_Pass
- * External Net= default
- * Firewall > Aliases > IP
 - * Name= HomeNet
 - * Type= Network
 - * Network= 172.30.2.0/24
- * Services > Snort > Pass Lists
 - * Name= HomeNet_Pass
 - * Assigned Alias= HomeNet



Snort in pfsense

/usr/local/etc/snort/snort.conf
/usr/local/etc/snort/rules/*.rules



簡報完畢 謝謝

