

ShareTech 眾至資訊

網路安全解決方案



大綱

- 網路安全攻防戰
- 網路行為分析理論
- 你有內部網路速度、管理及安全的問題嗎？
- ShareTech 的解決方案

網路安全攻防戰

網路安全攻防戰

- 面對網路安全攻防戰，哪一種網路架構是最安全的，我該買哪些設備呢？
- 不安全的來源
 - 1. 作業系統的漏洞。
 - 2. 應用軟體的漏洞：IE、Office甚至連 JPEG都有問題。
 - 3. 使用者不當的上網行為：點我賺大錢，結果被裝木馬。
 - 4. 惡作劇：NetCUT 網路剪刀手、IP/MAC 偽裝。
 - 5. 惡意的攻擊。

網路安全攻防戰

- 傳遞方式：網路
- 防護方式：網路產品安全進化論
- IP 分享器
- IP 分享器=>防火牆
- 防火牆 =>防火牆 + 防毒牆
- 防火牆 + 防毒牆 =>防火牆 + 防毒牆+入侵偵測。
- 達成目標：
可以預防95%的攻擊，不建立是死路一條。
- **最安全的網路安全**
- 剪掉網路線。

網路行為分析理論

使用者網路行為分析理論

- 如何由連線數來推論，使用者的網路行為是合理或不合理。
- **傳統方法**：不論是正常上網，被駭客攻擊、攻擊別人、被當跳板甚至中毒，要找到原因，必須將所有的網路封包攔截下來，組合、分析其內容，正常的封包放行，不正常的封包阻擋，在這個運作模式下，為了不影響網路速度，這樣的動作須要有快速的CPU，時時更新的特徵碼資料庫，耗時費力。
- **網路行為分析**：從網路的觀點來看，上述的行為都會變成TCP / UDP 的連線(Session)跟通訊埠(Port)，只要去統計所有IP/MAC 位址的TCP / UDP 的**連線數**、**通訊埠**跟**時間**的關係，就可以推論出使用者的網路行為，並進一步分析合理或是不合理的使用行為，不用去檢查封包內容，速度快價格又便宜。

理論基礎：蠕蟲、病毒、木馬的特徵值

- 不論是哪種木馬、病毒、蠕蟲，以 TCP/UDP 連線封包來分析，只要它的連線數超過設定的臨界值，就可以合理的懷疑是否有攻擊。
 - 1、某一來源IP，對不特定的目標IP執行相同的 Destination 通訊埠，例如：445 . 443 . 135 . 137。
 - 推測：這個來源IP已經中毒。
 - 2、某一來源IP，對特定的目標IP執行不相同的通訊埠，
 - 推測：這個來源IP在執行Portscan。
 - 3、不特定來源IP，對特定的目標IP，執行相同 Destination通訊埠，例如445.443.135…
 - 推測：這個目標IP正遭受攻擊。
 - 4、狂送出 TCP SYN 或 UDP SYN
 - 推測：想把目標IP的TCP或UDP buffers 佔完，藉以癱瘓主機或產生緩衝區溢位。

傳統的異常網路行為特徵值

- 以殺手病毒為例，經過數值分析後會歸納成下列的特徵值：

A、Sasser 病毒會要求送出SYN封包。

B、不特定的來源或目的IP位址。

C、目的PORT 為445。

D、來源PORT 不特定。

E、封包長度為48 Bytes。

F、當這類型的封包量達到 500 Packets/5 秒 = 100 Packets /秒

符合上述6個特徵時，ML-9280就會判斷遭受到Sasser 病毒的攻擊，Switch可以將有問題的網路使用者在感染的第一時間封鎖，讓它沒有機會再去感染其他人。

Worm Name	Sasser445
IP Protocol	TCP
TCP SYN	<input checked="" type="checkbox"/> 送出要求TCP SYN的封包
Destination IP	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> 不特定的來源及目的位址
Source IP	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Destination Port	445 目的 port 為445
Source Port	<input type="text"/> 來源 port 不一定
IP Length	48 每個封包資料長度為 48 bytes
High Flow	500 pkts/(5 seconds) < Lock by Physical port Rate 64K 超過 500p/5s ,ML-9280 封鎖這個埠
State	<input type="radio"/> Disabl

特徵值資料庫

- 除了系統預設的網路行為特徵值的偵測外，ML-9280也允許管理者依據自己公司的網路狀態，設定特徵值，如下表，讓網路更順暢穩定。
- 這些資料庫也可以匯入、匯出，讓管理者依據自己公司的網路環境調整適當的特徵值。

Export Worm to File		export							
Import Worm From File		瀏覽...							
Send Reset									
Action	Name	IpProt	Dport	Sport	Tcpsyn	Len	HiFlow	Feature	State
Delete Disable Edit	DEMO23	6	445	0	1	0	300	0	Enable
Delete Enable Edit	DdosDp135	6	135	0	1	48	500	MacFilter	Disable
Delete Disable Edit	MSBLAST135	6	135	0	0	92	500	0	Enable
Delete Disable Edit	MSBLAST2048	6	2048	0	0	92	500	0	Enable
Delete Disable Edit	MSBLAST5554	6	5554	0	0	92	500	0	Enable

有內部網路速度、管理及安全
的問題嗎？

內部網路的問題(一)

- 內部網路速度太慢，變成 Gigabit 的交換器後，狀況一樣，真正的速度瓶頸是：

交換機的交流頻寬不夠？

有人濫用？

廣播封包？。

- 內部網路的使用者偷改IP或是MAC位址，造成資安的漏洞。
- 一但有人中毒，如何在第一時間將電腦隔離？
- 如何防範未知的病毒、木馬攻擊？

內部網路的問題(二)

- 使用者偷改IP或是MAC位址
 - A、造成網路架構混亂、管理不便。
 - B、使用者用無線 AP 及 Notebook 私接網路造成資訊安全的漏洞。
 - C、防火牆有設IP/MAC位址管制，使用者一直更改IP/MAC，測試系統的漏洞，造成別人無法使用網路或是斷斷續續的現象。
 - D、故意癱瘓內部網路，使用MAC的攻擊軟體(如Netcut，網路剪刀手)。
- Layer 3 交換器太貴、用到的功能太少。
- 如何在第一時間找出有問題的電腦、並且將它隔離？