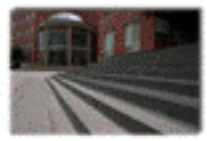
亞洲大學 | 資訊工程學系
Department of Computer Science and Information Engineering , Asia University




資訊安全防衛建置
網路防護設計及入侵偵測實作

亞洲大學 資訊工程學系　學生：謝佳洲
指導教授：周永振 教授

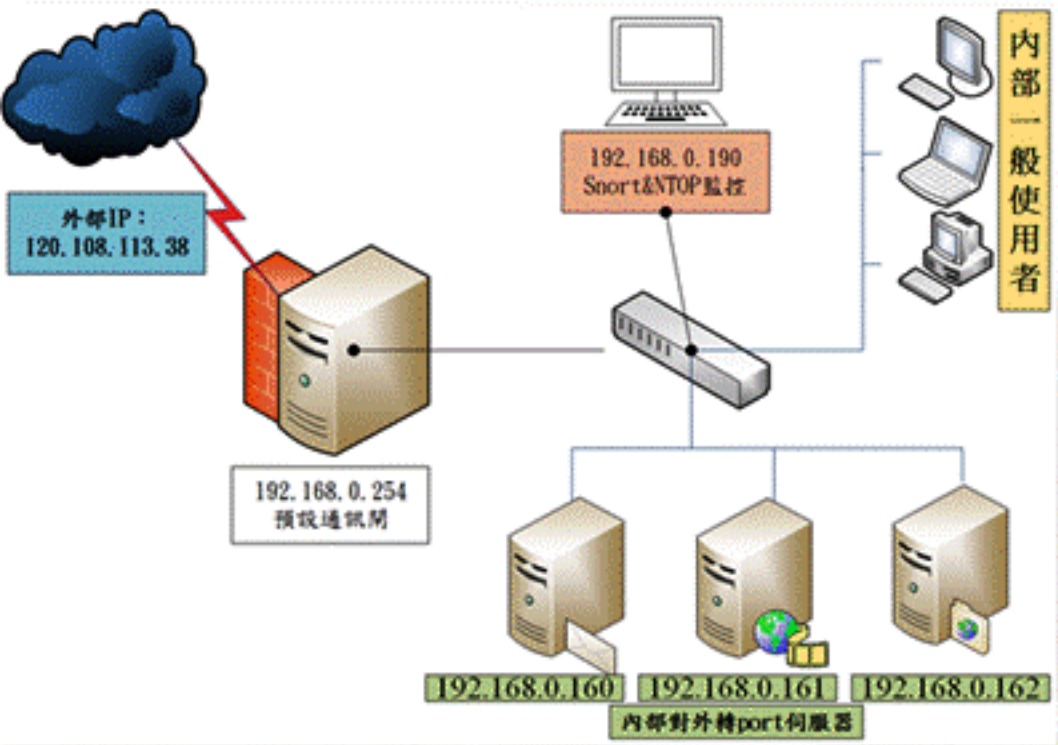
摘要

在網路發達的現今，為了防範資訊系統遭受入侵或攻擊，常會使用各種網路安全系統如防火牆以及入侵偵測系統建構防衛系統，然而以現今的技術及實際狀況，防衛系統仍需要管理者緊密的配合才能正確的阻斷攻擊，為了讓防衛系統能更為靈敏且自動化針對攻擊進行正確的防衛動作，本專題將設計與實作一個實用及安全性兼顧的防禦機制系統。

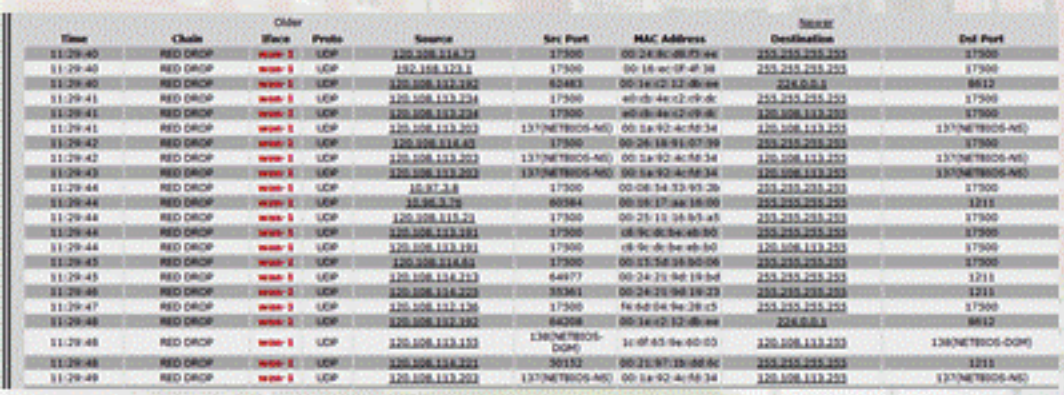
方法

(1) 機制推演：為了瞭解網路防護機制之設計是否適合目前網路安全環境，除針對各種假設進行推演，以確定專題實作方向與相關核心技術。

(2) 雛形系統實作：為證明本機制之可行性，我們著手實作系統雛形，挑選適合本機制使用之相關需求設備，進行防護機制與入侵偵測測試，並同步進行Freeware 軟體測試與攻擊測試。

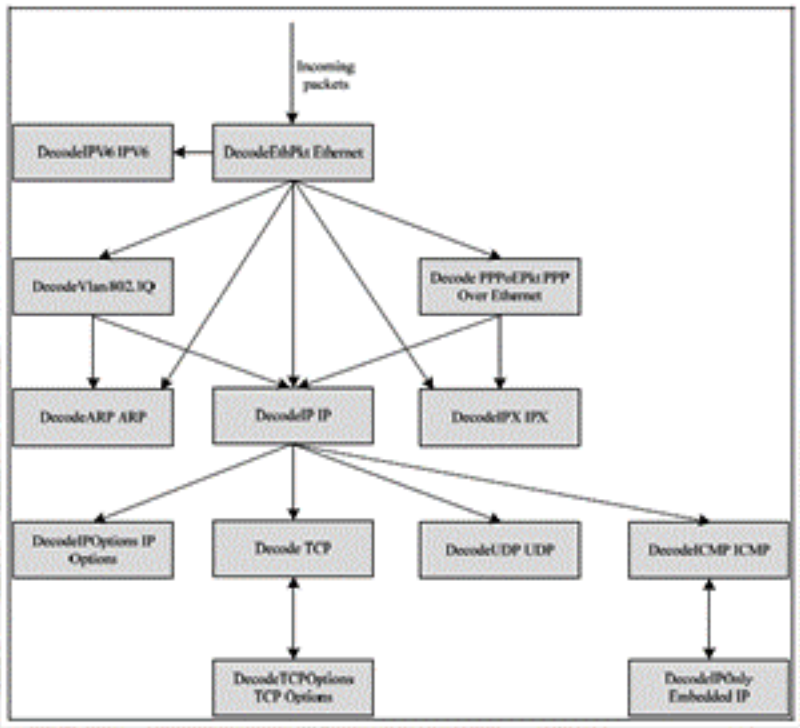


圖一、 網路架構雛形



Time	Chain	Older Iface	Proto	Source	Src Port	MAC Address	Newer Destination	Dst Port
11:29:40	RED DROP	wan-1	UDP	120.108.114.73	17500	00:24:8c:d8:f5:ee	255.255.255.255	17500
11:29:40	RED DROP	wan-1	UDP	192.168.123.1	17500	00:16:ec:0f:4f:38	255.255.255.255	17500
11:29:40	RED DROP	wan-1	UDP	120.108.112.192	62483	00:1e:c2:12:db:ee	224.0.0.1	9612
11:29:41	RED DROP	wan-1	UDP	120.108.113.234	17500	e0:cb:4e:c2:c9:dc	255.255.255.255	17500
11:29:41	RED DROP	wan-1	UDP	120.108.113.234	17500	e0:cb:4e:c2:c9:dc	120.108.113.255	17500
11:29:41	RED DROP	wan-1	UDP	120.108.113.203	137(NETBIOS-NS)	00:1a:92:4c:fd:34	120.108.113.255	137(NETBIOS-NS)
11:29:42	RED DROP	wan-1	UDP	120.108.114.43	17500	00:26:18:91:07:99	255.255.255.255	17500
11:29:42	RED DROP	wan-1	UDP	120.108.113.203	137(NETBIOS-NS)	00:1a:92:4c:fd:34	120.108.113.255	137(NETBIOS-NS)
11:29:43	RED DROP	wan-1	UDP	120.108.113.203	137(NETBIOS-NS)	00:1a:92:4c:fd:34	120.108.113.255	137(NETBIOS-NS)
11:29:44	RED DROP	wan-1	UDP	10.97.3.8	17500	00:08:54:53:93:2b	255.255.255.255	17500
11:29:44	RED DROP	wan-1	UDP	10.96.3.76	60384	00:16:17:aa:16:00	255.255.255.255	1211
11:29:44	RED DROP	wan-1	UDP	120.108.115.71	17500	00:25:11:16:b5:a5	255.255.255.255	17500
11:29:44	RED DROP	wan-1	UDP	120.108.113.191	17500	c8:9c:dc:8e:eb:b0	255.255.255.255	17500
11:29:44	RED DROP	wan-1	UDP	120.108.113.191	17500	c8:9c:dc:8e:eb:b0	120.108.113.255	17500
11:29:45	RED DROP	wan-1	UDP	120.108.114.61	17500	00:15:58:16:b0:06	255.255.255.255	17500
11:29:45	RED DROP	wan-1	UDP	120.108.116.213	64977	00:24:21:9d:19:bd	255.255.255.255	1211
11:29:46	RED DROP	wan-1	UDP	120.108.116.223	55361	00:24:21:9d:19:23	255.255.255.255	1211
11:29:47	RED DROP	wan-1	UDP	120.108.112.136	17500	fe:6d:04:9e:28:c5	255.255.255.255	17500
11:29:48	RED DROP	wan-1	UDP	120.108.112.192	64208	00:1e:c2:12:db:ee	224.0.0.1	9612
11:29:48	RED DROP	wan-1	UDP	120.108.113.153	138(NETBIOS-DGM)	1c:6f:65:9e:60:03	120.108.113.255	138(NETBIOS-DGM)
11:29:48	RED DROP	wan-1	UDP	120.108.116.201	50152	00:21:97:19:dd:6c	255.255.255.255	1211
11:29:49	RED DROP	wan-1	UDP	120.108.113.203	137(NETBIOS-NS)	00:1a:92:4c:fd:34	120.108.113.255	137(NETBIOS-NS)

圖二、 防火牆Log檔



圖三、入侵偵測程序封包處理

圖四、網路安全研究室　維運主機