Honeypot

Indice

1 Introduzione **2**
1.1 Kathara 2
1.2 Immagini Docker 2

2 Topologia della rete **2**

3 Spazio dei nomi **3**

4 Raggiungibilità **3**

5 LAN **3**
5.1 LAN A 3
5.2 LAN B 3
5.3 LAN C 4
5.4 LAN S 4
5.5 LAN D 4
5.6 LAN O 4

6 NAT **4**

7 Firewall **5**

8 Accounts **5**

1 Introduzione

Questo documento descrive l'architettura di rete utilizzata con Kathara per simulare un ambiente honeypot, consentendo l'analisi e lo studio di attacchi informatici in un contesto controllato. Il setup include vari dispositivi di rete e un server honeypot configurato per catturare e registrare le interazioni degli attaccanti.

1.1 Kathara

Per il seguente lavoro, è stata utilizzata Kathara, una piattaforma di simulazione di rete che consente di creare e gestire scenari di rete complessi utilizzando container docker. Kathara è particolarmente utile per l'insegnamento e la sperimentazione in ambito networking.

1.2 Immagini Docker

Nel laboratorio sono state usate delle immagini Docker custom fornite da theb0ys.

- theb0ys/base: Immagine base.
- theb0ys/apache: Server web Apache.
- theb0ys/VERSIONE ALTERNATIVA: Versione alternativa di Apache.
- theb0ys/samba: Condivisione file e stampanti.
- theb0ys/mariadb: DB MariaDB configurato per interfacce multiple.

2 Topologia della rete

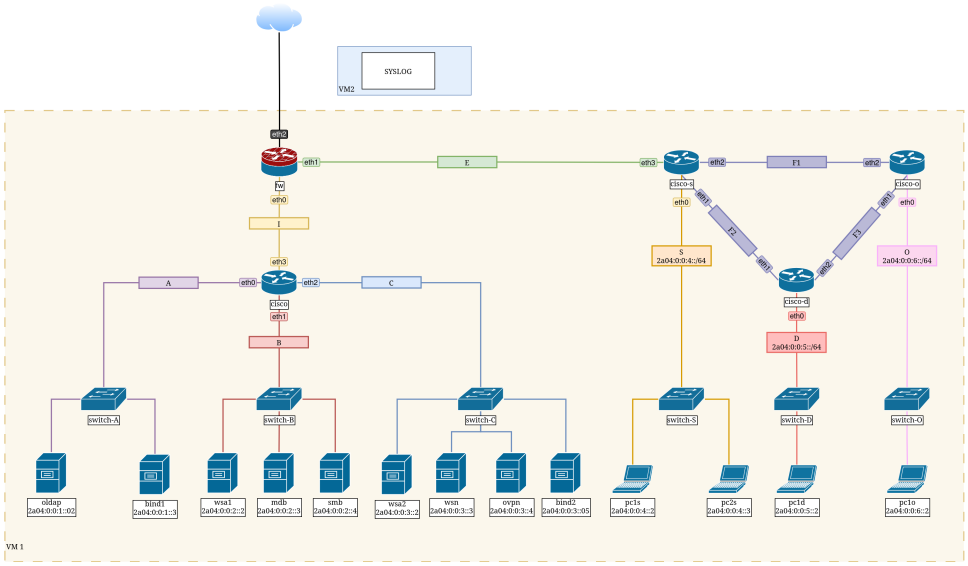

Figura 1: Topologia della rete

3 Spazio dei nomi

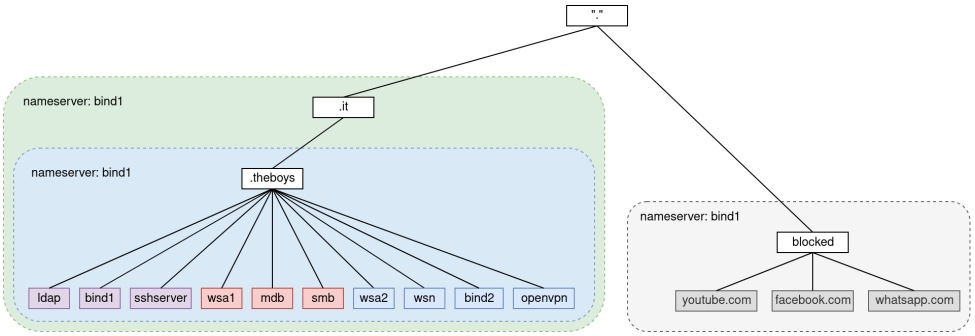

Figura 2: Namespace

4 Raggiungibilità

DA/A	LAN A	LAN B	LAN C	LAN D	LAN O	LAN S	Internet
bind1	V	V	V	V	V	X	X
oldap						X	X
wsa1	V	V	V	V	V	X	X
mdb					X	X	V
wsa2						X	V
nginx						X	V
openvpn						X	V
bind2	V	V	V	V	V	X	V
pcs1	V	V	V	V	V	V	V
pcs2	V	V	V	V	V	V	V
pcd1						X	V
pco1						X	V

5 LAN

5.1 LAN A

Descrizione: La lan A è ...
Router:
Hosts:

- ldap
- bind1: DNS server bind9, risoluzione per la intranet.

5.2 LAN B

Descrizione: La lan B è ...
Hosts:

- wsa1: Web server Apache2 interno.
- mdb
- smb

5.3 LAN C

Descrizione: La lan C è ...
Hosts:

- wsa2: Web server Apache2 con WP + MariaDB.
- wsn: Web server nginx per Internet.
- openvpn
- bind1

5.4 LAN S

Descrizione: La lan S è ...

5.5 LAN D

Descrizione: La lan D è ...

5.6 LAN O

Descrizione: La lan O è ...

6 NAT

Chain PREROUTING (nat) – Port Forwarding

#	target	prot	in	out	source	dest	src port	dst port	DNAT to	Note
1	DNAT	tcp	eth4		0.0.0.0/0	0.0.0.0/0	any	22	192.168.0.4:22	sshserver
2	DNAT	tcp	eth4		0.0.0.0/0	0.0.0.0/0	any	80	192.169.0.2:80	ws1a
3	DNAT	tcp	eth4		0.0.0.0/0	0.0.0.0/0	any	139	192.169.0.4:139	smb
4	DNAT	tcp	eth4		0.0.0.0/0	0.0.0.0/0	any	445	192.169.0.4:445	smb
5	DNAT	tcp	eth4		0.0.0.0/0	0.0.0.0/0	any	8080	192.170.0.3:80	wsn

Chain FORWARD – Allow NAT Traffic

#	target	prot	in	out	source	dest	src port	dst port	Note
1	ACCEPT	tcp			0.0.0.0/0	192.168.0.4	any	22	sshserver
2	ACCEPT	tcp			0.0.0.0/0	192.169.0.2	any	80	ws1a
3	ACCEPT	tcp			0.0.0.0/0	192.169.0.4	any	139	smb
4	ACCEPT	tcp			0.0.0.0/0	192.169.0.4	any	445	smb
5	ACCEPT	tcp			0.0.0.0/0	192.170.0.3	any	80	wsn

7 Firewall

Chain INPUT (Policy ACCEPT)

(Nessuna regola specificata)

Chain FORWARD (Policy DROP)

#	target	prot	in	out	source	dest	src port	dst port
2	ACCEPT	all			192.168.0.0/24			
3	ACCEPT	all			192.169.0.0/24			
4	ACCEPT	all			192.170.0.0/24			
5	ACCEPT	tcp			192.168.1.0/24			22
6	ACCEPT	all						

Chain OUTPUT (Policy ACCEPT)

(Nessuna regola specificata)

8 Accounts

SSH

Host	Username	Password	Tipo di Account
bind	senior	1Password!	Amministratore Senior
bind	junior	2Password!	Amministratore Junior
ldap	senior	1Password!	Amministratore Senior
mdb	senior	1Password!	Amministratore Senior
openvpn	senior	1Password!	Amministratore Senior
smb	senior	1Password!	Amministratore Senior
wsa1	senior	1Password!	Amministratore Senior
wsa1	junior	2Password!	Amministratore Junior
wsa2	senior	1Password!	Amministratore Senior
wsa2	junior	2Password!	Amministratore Junior
wsn	senior	1Password!	Amministratore Senior

wsn	junior	2Password!	Amministratore Junior

Samba

Host	Username	Password	Tipo di Account
smb	mario	1as-aoi	Dirigente
smb	filippo	lolw-9u!	Dipendente

DB / phpMyAdmin

Host	Username	Password	Tipo di Account
mdb	senior	1Password!	Amministratore Senior
mdb	junior	2Password!	Amministratore Junior
mdb	pluto	pluto	Da eliminare - funziona solo in v0.5-ufficiale in su