Miniguida su come consentire solo specifiche porte su Zeroshell

Nota: non raccomando l'uso di questo metodo per controllare l'accesso alle risorse di Internet da parte degli utenti della vostra LAN. Un utente un po' più furbo della media potrebbe configurare infatti un server VPN o SSH che risponda su una delle porte lasciate aperte, eludendo così il blocco. Allo stesso modo, alcuni software come Skype e TeamViewer sono progettati per tentare di superare gli eventuali firewall e quindi nel caso la loro porta specifica sia bloccata comunicano sulla porta 80 o 443, ignorando nuovamente le restrizioni che avete impostato.

Inoltre le regole potrebbero causare problemi per alcuni usi: ad esempio, se consentite solo le canoniche 80, 8080, 25, 110, 53 e qualcuno dovrà scaricare un file via FTP (porta 21), non potrà farlo. Idem se qualche programma usa una porta non-standard.

Detto questo, passiamo alla configurazione.

La rete di test che ho creato per questa miniguida è siffatta:

- Zeroshell fa da router, server DHCP e firewall e ha due schede di rete
- La scheda N°1 (eth00) è collegata ad un altro router e ottiene l'indirizzo via DHCP
- La scheda N°2 (eth01) ha come indirizzo 192.168.43.1/24
- La LAN che vogliamo filtrare è quindi 192.168.43.0/24

Tralascio la descrizione di come impostare la funzione di router e server DHCP in quanto ci sono già ottime guide sul web per configurarli :-)

Nella pagina "Firewall" **NON tocchiamo la "policy" mettendola su "DROP"** come verrebbe intuitivo fare! In questo modo ci si chiude fuori da Zeroshell (serve accedere fisicamente alla macchina e riavviare in failsafe mode)!

Supponiamo di voler consentire solo le porte 80, 443 e 53 (benvenuti nel 1984 ;-)). L'operazione è semplicissima.

Prima di tutto dobbiamo consentire l'accesso dalla LAN a Zeroshell, altrimenti ci chiudiamo fuori. Clicchiamo su "Add", si aprirà questa finestra.

<u>.</u>	Rule config - Mozilla Firefox – 🗆 🗙
(i) 172.16.31.64/cgi-bin/kerbyn	et?Section=FW&STK=542cd0a951bc26a6c76af673f398515e22e39557&Action=ChangeRule&Chain=FORWAR 🚥 又 💂 🏠 😑
FORWARD	Apply to Routed and Bridged Packets Sequence 1 + - Confirm Close
Description	Accetta Zerosheli
Packet Matching	Description Value Not Input • • Output • • Source IP (*) 192.168.43.0/24 • Destination IP 192.168.43.1 • Fragments [•••] match only second and further fragments] • Packet Length • • Source MAC • •
Connection State Not	NEW ESTABLISHED RELATED INVALID UNTRACKED
Time Matching	From V: V to V: V Mon Tue Wed Thu Fri Sat Sun
nDPI Deep Packet Inspection	Matching Not nDPI Manager
Layer 7 Filters	Protocol Description Not L7 Manager
DiffServ	DSCP
Connection Limits	Parallel connections per IP more 🔽 than Traffic per connection more 🔽 than MB 💌
ACTION	ACCEPT - Burst Burst
NOTES: (*) The IP addresses and IP range (ex. (**) TCP and UDP por	can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) 192.168.0.19-192.168.0.73) s can be single port (ex. 88) and port range (ex. 1903:1973)

- In "**Description**" mettete qualcosa che vi aiuti a capire la regola :-)
- In "**Source IP**" mettete la subnet della vostra LAN (qui **192.168.43.0/24**)
- In "Destination IP" mettete l'IP di Zeroshell (qui 192.168.43.1)
- In "Action" impostate ACCEPT.

Passiamo ora alla configurazione delle regole vere e proprie. Fate nuovamente clic su Add:

(i) 172.16.31.64/cgi-bin/kerbyn	at7Section=FW&STk=542cd0a951bc26a6c76af673f398515e22e39557&Action=ChangeRule&Chain=FORWAR 🚥 叉 🚊 🏠 📃
FORWARD	Apply to Routed and Bridged Packets 🚽 Sequence 1 + - Confirm Close
Description	Consenti 80
Packet Matching	Description Value Not Input Image: Constraint of the second and function of the second and further fragments Image: Constraint of the second and further fragments Source MAC Image: Constraint of the second and further fragments Image: Constraint of the second and further fragments
Protocol Matching Not	Source Port Not Dest. Port Not Opt Not Flags SYN ACK FIN RST URG PSH
Connection State Not	New ESTABLISHED RELATED INVALID UNTRACKED
Time Matching	
nDPI Deep Packet Inspection	Matching Not nDPI Manager
Layer 7 Filters	Protocol Description Not L7 Manager
DiffServ	DSCP
Connection Limits	Parallel connections per IP more 🝷 than Traffic per connection more 🝷 than MB 🝷
ACTION	ACCEPT - LOG 10 / Minute Burst 15
NOTES: (*) The IP addresses and IP range (ex. (**) TCP and UDP port	:an be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) 192.168.0.19-192.168.0.73) s can be single port (ex. 88) and port range (ex. 1903:1973)

- In "**Description**" mettete qualcosa che vi aiuti a capire la regola :-)
- In "**Source IP**" mettete la subnet della vostra LAN (qui **192.168.43.0/24**)
- In "**Protocol Matching**" selezionate **TCP** e impostate la porta che desiderate consentire nel campo **Dest. Port** (si può usare una porta singola tipo 80 oppure un range di porte come 1000:1200 ma NON tutti e due)
- Aggiungere, volendo, dei parametri di orario in "Time Matching"
- In "Action" impostate ACCEPT.

Aggiungete altre regole identiche per consentire ulteriori porte.

Allo stesso modo, per consentire le porte **UDP**, aggiungete regole identiche ma selezionate "**UDP**" in "**Protocol Matching**" anziché **TCP**.

A questo punto, dopo aver aggiunto tutte le regole che consentono l'accesso alle porte autorizzate, configuriamo una regola generale che blocchi tutto ciò che non rientra nelle regole precedenti.

Facciamo nuovamente clic su "Add".

- In "Source IP" mettete la subnet della vostra LAN (qui 192.168.43.0/24)
- In "Action" impostate DROP o REJECT. Consiglio di impostare REJECT. Il motivo di questa scelta è spiegato in quest'ottimo articolo: https://www.achab.it/achab.cfm/it/blog/achablog/drop-vs-reject-qual-e-la-differenza

Potete anche spuntare la casella "**LOG**" che registrerà tutti gli utenti che tentano di forzare il firewall.

Alla fine, si dovrebbe avere qualcosa di simile:

6		ZS:172.16.31.64 - Mozilla Firefox	- • ×
ZS:172.16.31.64	× +		
(←) → C ² (△) (○)	P 172.16.31.64	😇 🏠 🔍 Cerca 📃 👱 💷	5 @ ≡
ZEROSHELL The Services	Release 3.8.2 <u>About</u>	1.95 Kbit/s (Connections: 9 Load: 0%) (Vtop Cru (1) Anto Prycens 1600 six-Core Cru (1) Processor 3154Hitt : Logout Reboot Shutdown Utop 102551248 (9% used) Uptime 0 days, 0.45	Details Graphics
	FIREWALL	Manage 1.7 Filter Connection Tracking	
Alerts: None	Chain: EORWARD		ShowLog
SYSTEM	Save Cancel		Enabled
Setup	FORWARD Rules	Add Change	Delete
Logs	Seq Input Outp	ut Description	Log Active
Monitoring	1 * *	ACCEPT all opt in * out * 192.168.43.0/24 -> 192.168.43.1 /* Accetta Zeroshell */	no 🗹
USERS	○ 2 * *	ACCEPT tcp opt in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:80 /* Consenti 80 */	no 🗹
Users Groups	3 * *	ACCEPT tcp opt in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:443 /* Consenti 443 */	no 🗹
RADIUS	0 4 * *	ACCEPT tcp opt in * out * 192.168.43.0/24 -> 0.0.0.0/0 tcp dpt:53 /* Consenti 53 */	no 🗹
Accounting Captive Portal	5 * *	REJECT all opt in * out * 192.168.43.0/24 -> 0.0.0.0/0 reject-with icmp-proto-unreachable	no 🗹
NETWORK			
Hosts Router			
• DNS			
DHCP			
VPN OoS			
Net Balancer			
SECURITY Firewall			
HTTP Proxy			
• X.509 CA			
 Kerberos 5 			
	1		1
	May 02 17:55,19 SUCCE May 02 18:02.11 SUCCE	SS: Chain FDRWARD successfully saved.	
	- may 02 10.02,11 SUCCE		
	-		

A questo punto fate clic su **"Save"** e controllate che tutto funzioni. Se per caso vi siete chiusi fuori da Zeroshell, accedete fisicamente alla macchina e premete il tasto Z (fail-safe mode).

Ed ecco qui il risultato: la macchina collegata alla LAN riesce a navigare in Internet perché le porte 80, 53 e 443 sono aperte, ma non riesce ad accedere al server FTP perché la 21 è chiusa.

The as the transformed and the	
P Home Page Antro di Jacopo - Microsoft Internet Explorer	
ne Luk vew revolues toos hep	19 <u>0</u>
	■ 🗟 Co. Linke ≫
wariess en uch://www.a-cencaur.com/	
Intro di Jacopo	-
Benvenuti!	
Cosa troverete qui?	
Questo sito è nato come repository di risorse e howto per me stesso. Tuttavia h	o deciso di renderlo fruibile a t
nche perché certi argomenti trattati non sono facilmente disponibili su internet.	Qui troverete:
rticoli: recensioni, how-to, etc., sia nel campo informatico che elettronico.	
itorie: racconti, storie etc. (Non ancora disponibile)	
lepository: file rari e non, da scaricare.	-
(
<u>8</u>]	🔹 📝 Internet
tp://ftp.a-centauri.com/ - Microsoft Internet Explorer	_ 🗆 🗙
File Edit View Favorites Tools Help	
🔶 Back 🔹 🤿 🖈 🔂 🔯 Search 🖓 Folders 👹 History 🛛 🎬 🎇 💥 🖄 🧱 🕶	
Address 😰 ftp://ftp.a-centauri.com/	▼ 🔗 Go 🛛 Links ≫
FTP Folder Error	
An error occurred reading the contents of the folder. Make sure the file name is valid and y	ou have permission to access the location
Details:	
A connection with the server could not be established	
OK	
Liser: Apopymous	Internet

Tutto qui :-)