IpFire RouterFirewall-IPS

La distro Gnu/Linux Ipfire fork del progetto **ipcop** è una soluzione orientata per soluzioni router/firewall con una intuitiva interfaccia grafica da remoto tramite https per la gestione, l'abilitazione di servizi da attivare e da aggiungere tramite plug-in installabili.

La **sicurezza informatica** è la priorità centrale dietro al progetto che, migliorato da un processo di *harding* interno al sistema, impedisce gli attacchi mirati al suo interno. Progetto **OpenSource** sviluppato sotto licenza GPL, ha alle spalle un'attivissima comunità di utenti e sviluppatori che hanno creato, dietro alla distro, la soluzione alle richieste più frequenti per uso sistemistico. IpFire è un software gratuito sviluppato da una vasta **comunità aperta**, esso è considerato affidabile da moltissimi utenti considerata la filosofia Opensource in cui ogni persona del comparto IT può visionare il codice sorgente, integrarlo e migliorarlo per rendere il progetto più innovativo.

Rilevante è la cura per il kernel con la protezione grsec e – nelle recenti versioni – la minimizzazione dagli attacchi Meltdown e Spectre legati ai processori intel. Il sito web (ipfire.org) contiene forum e blog a servizio della comunità. IpFire applicato ad un PC con due schede di rete e una wifi può funzionare da routerFirewall, routerwifi o access point con funzioni di proxy e sistema IDS/IPS tramite l'uso di snort per bloccare attacchi mirati alla rete LAN da parte della WAN. Dal terminale del pc è possibile usare il gestore di pacchetti pakfire per installare e rimuovere software o monitorare con *tools* come htop, iotop o tshark.

L'**installazione** viene guidata da un susseguirsi di step per il settaggio della macchina dove, al termine, sarà possibile amministrare sia da riga di comando tramite *root* sia tramite interfaccia web https. La varietà dei menù permette il

monitoraggio del traffico in uscita e entrata e le connessioni con possibilità di storage di log e intuitivi grafici a torta. Ipfire non è una soluzione solo per uso firewall ma anche come BackupPc, client torrent e server multimediale interno per lo streaming.

Il punto di riferimento della comunità è all'indirizzo web (community.ipfire.org) dove discussioni raggruppate per *tool* e argomento permettono di ottimizzare e rendere questo progetto OpenSource sempre più famoso. Vi è un portale italiano di appassionati per solo **utenti italiani** (ipfireitalia.it) dove chiedere aiuto per chi è alle prime armi nella questioni di protocolli TCP/IP.

Apprezzatissimi sono gli **aggiornamenti frequenti** che mantengono forte IPFire contro vulnerabilità di sicurezza e nuovi vettori di attacco. Funzionalità quali QoS, proxy web e VPN permette il filtraggio dei contenuti web consentendo solo ad alcuni utenti la navigazione, resa più veloce tramite la memorizzazione cache delle pagine web. Clamav, associato al proxy, permette di eseguire la scansione trasparente dei virus e bloccarli prima che infetti i pc windows/Macosx della lan.

Le funzioni associabili al proxy web permettono anche il controllo degli accessi e la registrazione.

L'uso della **crittografia** più recente per OpenVPN, IPsec e https permette di garantire connessioni sicure, sia su internet che alla postazione ipfire. Nella sezione download (ipfire.org/download/ipfire-2.23-core138) si possono scaricare le iso e flash image per le architetture più utilizzate.

Per un aiuto professionale per consulenze specifiche c'è la lightning wire labs che prevede l'assistenza per un uso business; per i restanti nerd c'è l'apposito wiki

(wiki.ipfire.org).

Nella ultima release (core138) in cui scrivo questo articolo, IpFire si affretta a risolve e mitigare le vulnerabilità recentemente annunciate nei processori Intel.

Per chi volesse **contribuire al progetto TOR,** la comunità mette a disposizione il pacchetto installabile tramite pakfire per realizzare un punto di entrata al deepweb o anonimato per la rete lan o contribuire alla rete globale tor avviando un server Tor relay. La varietà degli strumenti messi a disposizione dalla distro permette di alzare le difese di una rete lan e utilità per il sistemista IT.

La funzione proxy cache offline associato alle blacklist (anche classificate in base alla nazione) permette di ottimizzare e risparmiare il traffico dati passante. Per chi volesse contribuire nello sviluppo del codice a questo link (wiki.ipfire.org/devel) è possibile trovare tutti i riferimenti necessari. Essendo un progetto OpenSource si sostiene con donazioni a sostegno da parte della comunità, un progetto che fin dagli inizi ha riscosso molti consensi positivi da parte di amministratori di rete ed esperti di pentest. Linux come sempre è il sistema operativo principale per chi ha sposato la filosofia opensource e free. La filosofia linux permette la modellazione del sistema operativo per gli **usi più svariati**, dai microcomputer ai supercomputer.

Il supporto Hardware associato al kernel linux sempre in aumento, la ricerca e sviluppo del software, la sicurezza *by design* e la privacy *by default* del progetto rende questo progetto un ottimo punto di riferimento, in ogni tipo di scenario, per proteggere da eventi di *data breach*.

Articolo a cura di **Fabio Carletti aka Ryuw**

Fabio Carletti aka Ryuw è un White Hat del gruppo (SoldierX Hacker team).

Noto ai più per questioni legate alla Sicurezza Informatica ha ottenuto importanti apprezzamenti in attività investigative per conto di Carabinieri e Polizia Postale. Dal 98 si occupa del mondo gnu/linux come security IT evangelist. Collabora come membro nel Tor Project team e nella Linux Foundation.

Ospite di rilevanti eventi italiani riguardanti la privacy, linux/unix, hacker camp e software open source dedica le sue energie alla ricerca nella sicurezza informatica.

https://www.ictsecuritymagazine.com/articoli/ipfire-routerfirewall-ips/