



Per Principianti

TEST YOUR IPS

Pierpaolo Palazzoli Fabio Mostarda

Grado di difficoltà



Per poter comprendere meglio le finalità del testing di un IPS, bisogna avere chiare le funzionalità peculiari di un IPS. Un Intrusion Prevention System è un sistema di sicurezza che è finalizzato a Bloccare i tentativi di intrusione, evitando esecuzione di codice remotamente su applicazioni di rete, conseguentemente privilege escalation di sistemi.

Mitiga enumerazione delle porte, Network vulnerability assessment e fingerprint. *DOS mitigation* evitando interruzione momentanea o continuativa dei servizi tramite flooding di traffico. *Ricostruzione delle sessioni TCP e UDP* e loro normalizzazione, per evitare frammentazione e attacchi sulla finestra di comunicazione.

Uno dei prerequisiti fondamentali per il testing di IPS è quello di configurarlo esattamente come si vorrebbe mandarlo in produzione, quindi le logiche sono:

- conoscere perfettamente la topologia dell'architettura del traffico e della rete, conoscere il numero e il tipo dei *server/client* che si intende proteggere, conoscere le applicazioni che vengono fruite dagli host protetti.

Eseguita quindi la configurazione dell'IPS in coerenza al contesto di rete dove deve essere applicato, è necessario distinguere la tipologia di blocco che si vuole testare. Di fatti gli IPS possono essere implementati in in due modi:

- In line ed Active response

Nel primo metodo il dispositivo si interpone tra la rete *buona* e quella *cattiva* di modo da poter analizzare tutto il traffico passante. Questo per poi arbitrariamente al processo di analisi di bloccare il traffico che, in coerenza con le rules, è ritenuto maligno. (Fig.1) Il secondo metodo è composto da una parte di analisi, quindi una interfaccia di rete dedicata all'analisi di rete senza stack TCP/IP, collegata ad una span port di uno switch, un Network TAP o Traffic redirection (Juniper), in grado di analizzare tutto il traffico passante nel segmento di rete delineato come zona da proteggere, la seconda rete con lo stack TCP/IP usata dal processo IPS per lanciare Reset in caso di connessioni TCP maligne e ICMP network un-

Dall'articolo imparerai

- Test stress di IPS.
- Analisi delle performance di un IPS.
- Tuning configurazionale di un IPS.

Cosa dovresti sapere

- Minima conoscenza di linux.
- Configurazione, installazione, gestione di un ips

reachable in caso si sessioni udp. La seconda modalità risulta meno precisa per attacchi di piccole dimensioni di pacchetto UDP (Fig.2).

Quindi le decisioni implementative risultano precedenti alla fase di testing, di modo da adoperarsi direttamente sul vero ambiente di sicurezza che verrà portato in produzione, solo esclusivamente dopo un prima fase nella quale le regole applicate saranno messe in IDS mode per la prima fase di rodaggio, per la scrematura dei falsi positivi più grossolani.

Finalità del benchmark

L'attività di benchmarking dell'infrastruttura IPS risulta fondamentale per comprendere due aspetti:

- il grado di protezione che offre la soluzione IPS prescelta (*Am I using the right IPS?*)
- il corretto dimensionamento del sistema IPS rispetto al traffico di rete (*Am I using the IPS right?*)
- Solo mediante una prova reale si potrà validare la soluzione tecnologica prescelta.
- I fattori di protezione dei quali verificare le prestazioni sono molteplici, ad esempio:

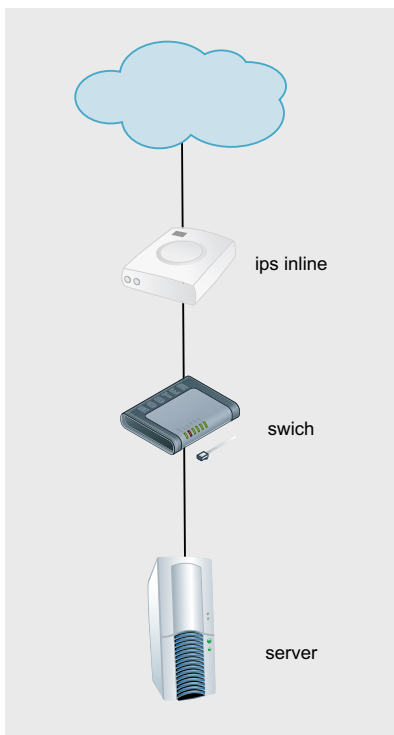


Figura 1. il traffico maligno

- resistenza e mitigazione di DoS
- mitigazione ping sweep
- rilevamento covert channel (tunnel in traffico HTTP, ICMP, etc...)
- mitigazione propagazione di worm noti
- comportamento in presenza di tunnel SSH/SSL.

Un aspetto fondamentale del benchmark è la determinazione della composizione del traffico da esaminare: la CAIDA (Cooperative Association for Internet Data Analysis) ha stimato che l'85% dei pacchetti ed il 92% dei byte siano traffico TCP, mentre il 12% dei pacchetti e il 5% dei dati siano UDP (principalmente DNS e RealAudio), con una dimensione media dei pacchetti stimata tra 413 e 417 byte. Il traffico rimanente è un misto di IP encapsulated, ICMP, GRE ed altri protocolli meno diffusi.

In secondo luogo si deve tener conto della latenza massima accettabile durante il test: essendo il throughput TCP dato dal rapporto tra window size e RTT (Round Trip Time), l'aumento della latenza può causare una diminuzione del throughput. Questo comporta conseguenze non banali:

- una latenza *one way* di 2 ms introdotta da un dispositivo IPS con una window size di 64 KB su una rete da 1ms di latenza, comporterà un aumento del RTT a 9 ms e si avrà un decadimento da 512 Mbps a 57 Mbps. Le misure non devono inoltre essere fatte su burst di dati ma su flussi stabili, così da neutralizzare l'effetto buffer intrinseco nell'IPS.

Si dovrà inoltre verificare la tenuta del sistema di fronte ad un numero di ses-

sioni simile a quello dell'infrastruttura reale. Avere una misura oggettiva di questo tipo di variabili può far emergere per tempo la necessità di hardware più performante (in termini di pura potenza grezza o mediante opportuni circuiti ASIC). Ci si dovrà infine sincerare che le regole attivate sull'IPS non blocchino alcun tipo di traffico legittimo: in fase di benchmarking, sarà possibile evidenziare quali flussi vengano interessati da fenomeni di questo tipo, predisponendo per tempo adeguate contromisure. Per realizzare questo, è opportuno che l'IPS sia messo di fronte al vero traffico della rete che dovrà in seguito proteggere; le soluzioni che permettono questo test sono molteplici, e tra queste:

- effettuare un mirroring del traffico di rete, ad esempio con l'utilizzo di un matrix switch layer 1 o di redirectione di traffico (feature presente sui alcuni prodotti Juniper Networks).
- utilizzare un software specifico per catturare traffico di rete e reimmetterlo (anche molteplici volte) nel sistema di test.

E' essenziale in questo tipo di prove rispettare la bidirezionalità del traffico:

- l'IPS dovrà sentire i dati fluire attraverso le opportune interfacce di rete; in caso contrario, si rischia di ottenere risultati anomali e fuorvianti.

Strumenti necessari

Per avviare la fase di benchmarking sarà quindi necessario avere:

- un IPS
- un sistema in grado di generare opportuno traffico di rete (bidi-

Listato 1. PCAP

```
Beginning test
Completed 1 loop of trace sample.pcap
Completed 1 loop of trace sample.pcap
Finished 2 loops of trace sample.pcap Completed: 1, Timed out: 0
Retrans: 0
Sent: 3458
Recv: 3458
```



reazionale) o di replicare traffico preventivamente catturato.

- una lista di test da eseguire, comprendente gli attacchi più comuni e qualche specifica variante (ad esempio, traffico malevolo rilevato sulle proprie reti).

Essi andranno poi opportunamente connessi, ad esempio come illustrato in Fig 3. *Tomahawk* Tomhawk è un software in grado di replicare traffico di rete (salvato mediante tcpdump o simili) a velocità arbitrarie; le sue caratteristiche salienti sono:

- Trace con 1000 TCP connection setup
- Replay di 250 copie di tracce in parallelo
- Fino a 31,000 connections/sec

Questo garantisce la possibilità di ripetere i test con precisione, non-

chè di amplificare attacchi sample un numero arbitrario di volte, così da portare l'IPS a confrontarsi con situazioni estreme. I requisiti minimi hardware di Tomahawk sono:

- Pentium ad almeno 1GHz
- RAM 512 MB
- Red Hat Linux 7.2 o successiva
- Due (2) gigabit Network Interfaces Cards (NICs), da assegnare a eth0 e eth1.
- Una (1) NIC per il management, da assegnare alla eth2

L'installazione del tool non è automatica, in quanto si dovranno seguire alcuni passi per effettuare il setup di NFS e per settare alcune variabili d'ambiente: tutto è comunque spiegato con estrema chiarezza nella homepage di Tomahawk.

Una volta completato il setup dell'applicazione, il suo utilizzo sarà

immediato: pensando di disporre di un sample di traffico d'interesse, il comando da shell sarà: # tomahawk -l 2 -f sample.pcap il quale riprodurrà due volte il file sample.pcap, ottenendo:

E' possibile inoltre forzare l'IP sorgente e di destinazione che verranno immessi nella rete di benchmark mediante operazioni di riscrittura degli header IP; questa caratteristica permette, disponendo di un numero sufficiente di sample di attacchi e traffico reale, di effettuare benchmark incredibilmente reali e di monitorarne lo status.

Nessus + (TOR + socat)

E' ben noto a tutti il funzionamento di nessus come strumento di Network Vulnerability assessment. L'applicazione di tale strumento risulta necessaria per molteplici motivi, uno dei quali è il testing delle vulnerabilità prima e dopo l'inserimento dell'IPS, l'effettivo funzionamento dell'IPS in modalità di blocco, testing su DOS.... La modalità standard di funzionamento però risulta estremamente limitante dato che la sorgente del test risulterebbe singola; per introdurre l'aspetto di multi provenienza e anonimato risulta molto utile utilizzare questo strumento tramite Tor.

In prima battuta installare Tor in ascolto sulla porta 9050 nel file di conf torrc: SocksPort 9050.

A questo punto l'obiettivo è far passare i test attraverso questo socket, lo strumento necessario si chiama socat, in grado di fare socket redirection, creerà quindi un connettore locale tra tor e la porta di destinazione del server protetto dal nostro IPS da testare. # socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1:10.0.0.1:80,socksport=9050

Il comando socat in questo caso redirige il traffico sulla porta 8080 in locale (127.0.0.1) verso la porta 80 del server 10.0.0.1 attraverso il socket 9050.

A questo punto basterà configurare il client di nessus affinché l'host da scansionare sia il 127.0.0.1 e la

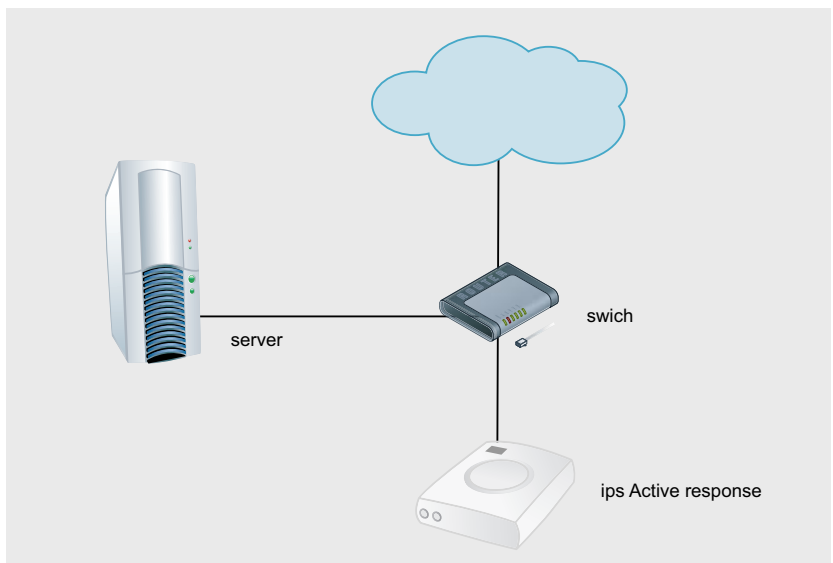


Figura 2. Attacchi di piccole dimensioni di pacchetto UDP

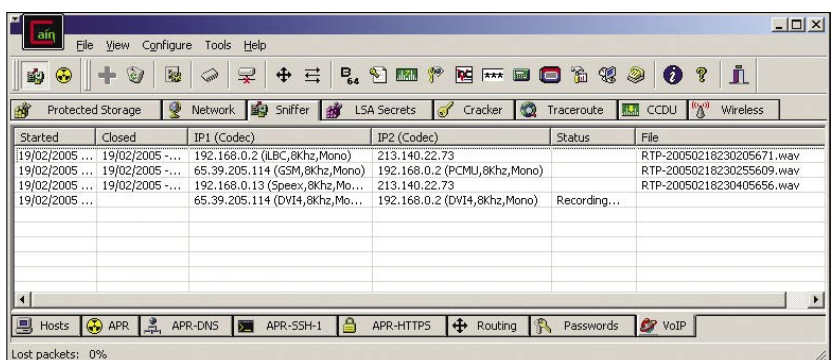


Figura 3. Sniffer

porta 8080 nella sezione Scan Options. Fig 4.

Quindi l'obiettivo rimane atteso, e l'assessment attraverserà la rete tor per raggiungere la destinazione così che il test di blocco sia più efficace e variegato. L'unica limitazione è la banda con la quale vengono fatti i test, che risulta limitata da tor stesso e il numero di porte da testare sarà esclusivamente una alla volta.

Da questa fase di test verranno prodotti report, prima e dopo l'introduzione dell'ips in modo da conoscere in maniera efficace e univoca il beneficio dell'introduzione di tale dispositivo, si conoscerà la reale capacità di blocco e attivando e disattivando correttamente le regole sia di nessus che dell'IPS di comprenderanno quali siano le configurazioni necessarie ed efficaci al contesto di rete protetto.

Mgen

Mgen è un software in grado generare traffico TCP/UDP finalizzato all'analisi delle performance di rete. La sua configurabilità è in grado di dare all'operatore la possibilità di scegliere parametri dei pacchetti fondamentali come TTL e TOS. Ormai alla versione 4 il pacchetto è scaricabile sia in sorgente che in binario.

Risulta molto intuitivo l'approccio configurazionale a script. Oltre a questa modalità esiste il funzio-

namento direttamente da linea di comando:

```
# mgen port 5000,5004-5006
    output log.drc
# mgen input script.mgn
```

Per un efficace testing risulta molto comodo la funzionalità di logging in invio. Questa funzionalità permette di registrare i dati in partenza in formato tcpdump. Infatti la ricezione del flusso, dopo essere passato nell'IPS, potrà essere registrata sempre da uno strumento tcpdump compatibile di modo da poter confrontare i file di trasmissione con quelli di ricezione. Questo permetterà una analisi dettagliata del trattamento dei pacchetti, tempi di risposta, modifiche dei flussi UDP e TCP. Guardando più in dettaglio uno script di esempio, mgen genererà un flusso UDP sulla porta 21 verso l'host 10.0.0.1 con dimensione pacchetto 1024 e rate di un pacchetto al secondo. PERIODIC significa che mgen genererà traffico periodico secondo le regole un pacchetto al secondo da 1024: 0.0 ON 1 UDP DST 10.0.0.1/21 PERIODIC [1.0 1024]

L'obiettivo dell'uso di Mgen di un benchmark di un IPS è quello di trovare in prima battuta il limite massimo di banda passante di un IPS configurato già per essere messo nel proprio contesto di rete. Il limite deve essere testato sia in TCP che in UDP. Questo perché la natura dei protocolli e delle configurazioni degli ips permette l'analisi e il riassetto di entram-

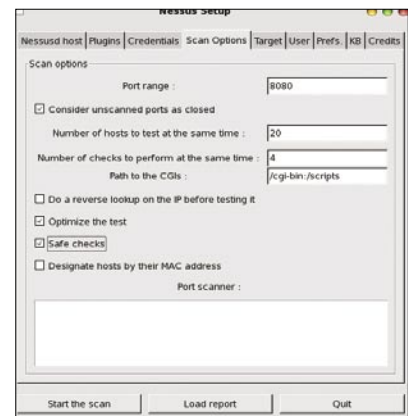


Figura 4. Port scanner

be le tipologie di flussi, creando così un limite software/hardware al passaggio di traffico. Essere consapevoli del limite del proprio dispositivo risulta estremamente importante ai fini del dimensionamento del segmento di rete che si vuole proteggere.

Un'altro fine all'uso di un traffic generator attraverso un IPS è di sicuro la configuration tuning necessaria, che altrimenti dovrebbe essere fatta in produzione.

Quindi necessario conoscere il contesto di rete da proteggere in termini di tipologia di traffico di modo da poter riprodurre condizioni le più simili possibili. Molte volte questi tipi di test vengono sottovalutati, ma più un dispositivo in line deve processare pacchetti, più tale dispositivo introdurrà tempi di latenza necessari all'inspection del pacchetto stesso. Essere a conoscenza di questi dati permette di fare le giuste considerazioni *tecniche/* economiche sull'IPS stesso.

Conclusione

Il benchmarking di uno strumento IPS risulta fondamentale per garantire l'adeguatezza della scelta di uno strumento IPS sia in fase di setup, validandone la configurazione e la funzionalità sulla base di specifiche reali, sia in fase di esercizio, ottenendo feedback concreti della sua capacità di protezione; in entrambi i casi, si avrà anche il benefico effetto collaterale di approfondire la conoscenza dello specifico IPS nonché della problematiche della rete da proteggere, con ricadute positive sulla qualità globale del servizio offerto. ●

Sull'autore

Snortattack.org, Portale orientato alla sicurezza informatica, è il risultato della fusione di conoscenze e collaborazione del team. Le tipologie di argomentazione trattate coprono 360 gradi tutte le tematiche relative alla sicurezza: *attacco/difesa*.

Grande punto di forza è l'uso di Snort come soluzione alle innumerevoli problematiche di intrusione. Per tenere gli utenti aggiornati sulle nuove problematiche sono a disposizione un forum e una mailinglist. Con Snortattack.org, si intende creare uno Snort User Group finalizzato alla collaborazione per l'Italia e tutto il resto del Mondo, per l'uso di Snort e la trattazione di problematiche di security.

In Rete

- <http://www.tomahawktesttool.org/>
- <http://pf.itd.nrl.navy.mil/mgen/mgen.html>
- http://www.oreillynet.com/onlamp/blog/2005/07/launching_attacks_via_tor.html