IPS challenge il gioco ... IN SCATOLA

snortattack.org

- Portale dove le tipologie di argomentazione trattate coprono a 360 gradi tutte le tematiche relative alla sicurezza: attacco/difesa.
- Uso di Snort come soluzione alle innumerevoli problematiche di intrusione.
- Un portale e una mailinglist.
- Snort User Group finalizzato alla collaborazione per l'uso di Snort e la trattazione di problematiche di security.

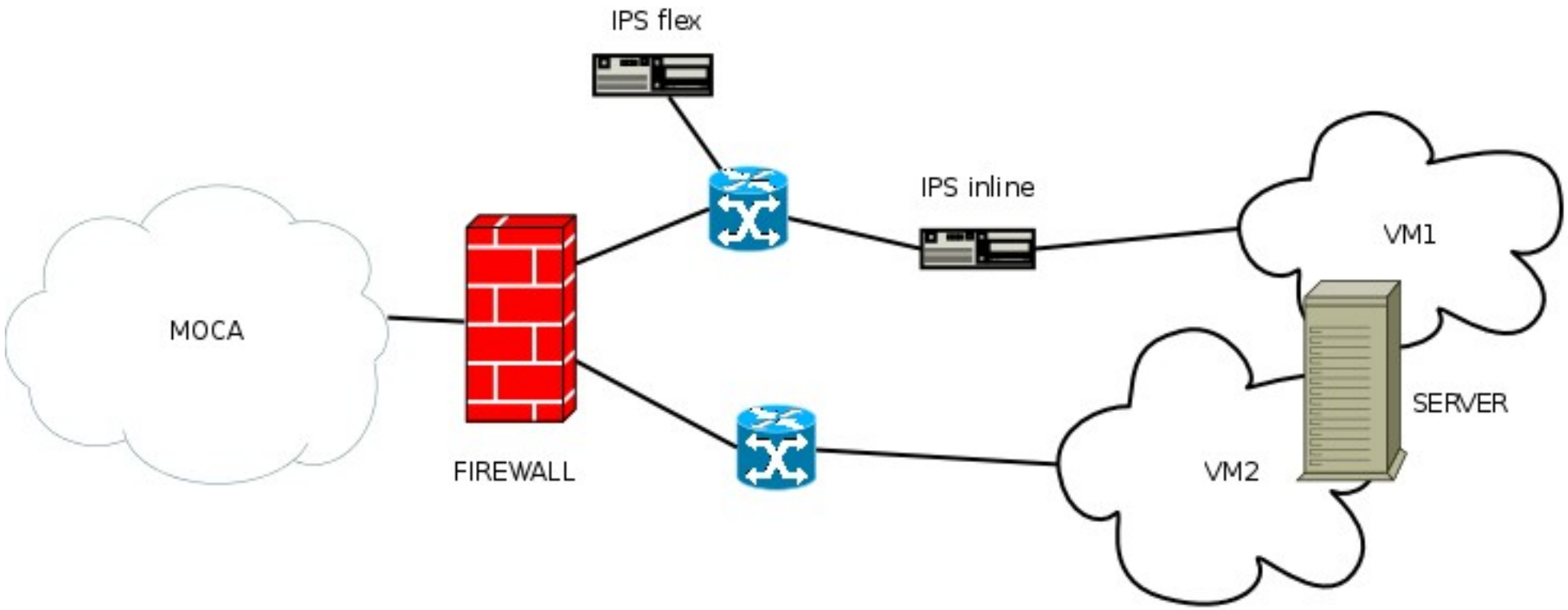
Idea di ips challenge

- GRANDI PREMI
  - SENZA IPS
    - Defacciamento sito → applausi
    - Root → PPCNM
  - CON IPS
    - Defacciamento sito → adesivo + maglietta
    - Root → felpa

Infrastruttura

- Firewall
- IPS in_line
- IPS flex
- Server ospitante 2 macchine virtuali UML (User Mode Linux) “quasi identiche”
  1. VM1 protetta da IPS
  2. VM2 senza protezione
- Switch Managiable

Schema semplificato

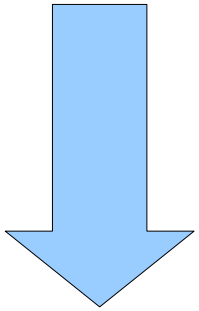


Firewall

- 2 ip attestati sulla rete MOCA
- Per ogni IP la Porta TCP 80 e' aperta verso le vm interne
- IP 172.16.0.12:80 → vm1:80 (con ips)
- IP 172.16.0.13:80 → vm2:80

moca-VM1 e moca-VM2

- Server web con interfaccia di rete dedicata
- CMS -> Joomla! e PHP-Nuke di versioni datate e non aggiornate



IL “PARCO GIOCHI”
PER QUESTO EVENTO !!!

snortattack
True security

FS per le vm UML

- Ogni macchina UML ha un filesystem di partenza base con il sistema funzionante (root_fs)
- COW copy on write → file traccia di tutte le modifiche verso il root_fs
- All'avvio
  - il root_fs viene utilizzato in ro
  - file COW aggiuntivo di tipo sparse per ogni vm
- Il ripristino alla situazione iniziale e' banale

snort

- Snort è un NIDS open source rilasciato con licenza GPL
- Analizza i pacchetti che transitano in rete, confrontandoli con un database di firme di attacchi
- Verifica e allerta (=Detection) eventuali anomalie relative al traffico di rete
- Possiede un database di attacchi aggiornabile tramite internet

snort in modalita' inline DROP

- Il sistema viene inserito in maniera trasparente tramite due schede di rete in bridge
- snort in questa modalita' ottiene i pacchetti da una coda (queue) di iptables tramite la libreria libipq anziche' dalla classica libpcap
- I pacchetti possono essere fermati (drop) o passati (pass) in base alle rules di snort

snort flex response RESET

- Snort in modalita' flex response permette di resettare le connessioni ritenute pericolose
- Prima interfaccia viene collegata alla porta in monitoring dello switch (porta dove vengono replicati tutti i pacchetti diretti ad una seconda porta dello switch che si vuole monitorare)
- Seconda int in rete per inviare i RST (o ICMP unreachable nel caso di pacchetti UDP) sia sulla porta del SRC che DEST per troncare la connessione

snort.conf

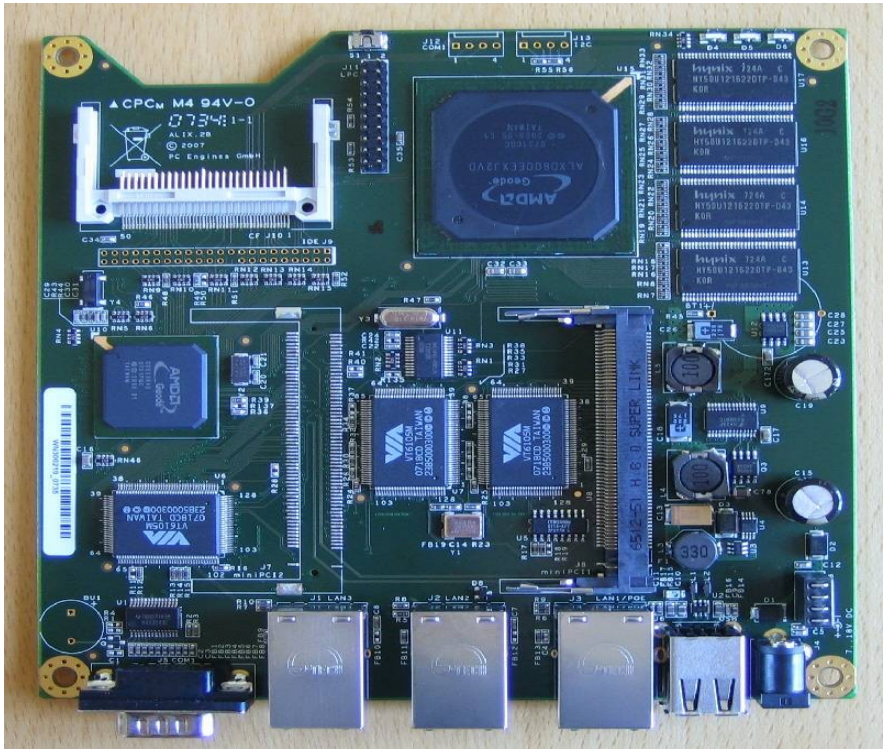

```
var HOME_NET [192.168.123.0/24]
var EXTERNAL_NET !$HOME_NET
var HONEYNET $HOME_NET
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var TELNET_SERVERS $HOME_NET
var SNMP_SERVERS $HOME_NET
var SSH_PORTS 22
var HTTP_PORTS 80
var SHELLCODE_PORTS !80
var ORACLE_PORTS 1521
var RULE_PATH /etc/snort/rules


config detection: search-method lowmem
preprocessor stream5_global: max_tcp 262144, track_tcp yes, track_udp yes
preprocessor stream5_tcp: policy first, use_static_footprint_sizes
preprocessor stream5_udp: ignore_any_rules
preprocessor http_inspect: global iis_unicode_map unicode.map 1252
preprocessor http_inspect_server: server default profile all ports { 80 8080 8180 }
oversize_dir_length 500 flow_depth 0

include $RULE_PATH/mysql.rules

...
```

rules

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET
any(msg:"PORNdildo";content:"dildo";nocase;flow:to_clie,
established; classtype:kickass-porn;
sid:1781;rev:1;resp:reset_both,icmp_all;)
```

```
drop tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"PORN hardcore anal";
content:"hardcore anal"; nocase;
flow:to_client,established; classtype:kickass-p
orn; sid:1311; rev:5;)
```

Hw utilizzato



Alix2c3
CPU: 500 MHz AMD Geode LX800
DRAM: 256 MB DDR DRAM
Storage: CompactFlash socket
Connectivity: 3 Ethernet channels
Expansion: 1 miniPCI slot, LPC bus

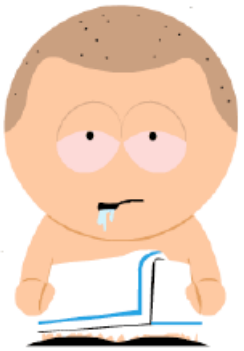
Static binary

- Snort compilato in modalita' statica
- Binario di dimensioni maggiori a causa dell'inclusione delle funzioni date dalle librerie necessarie al suo funzionamento
- L' esecuzione risulta velocizzata
- Il Deploy risulta semplificato (un solo file)

- http://www.snortattack.org/static/...
  - Snort_flex
  - Snort inline

Domande ....

Indovina chi ?



Documentazione

- http://www.snortattack.org
- http://snort.org/
- http://www.emergingthreats.net
- http://www.inliniac.net
- http://snort-inline.sourceforge.net/