Un Honeypot per domarli, un Honeypot per trovarli, un Honeypot per ghermirli e nel buio incatenarli

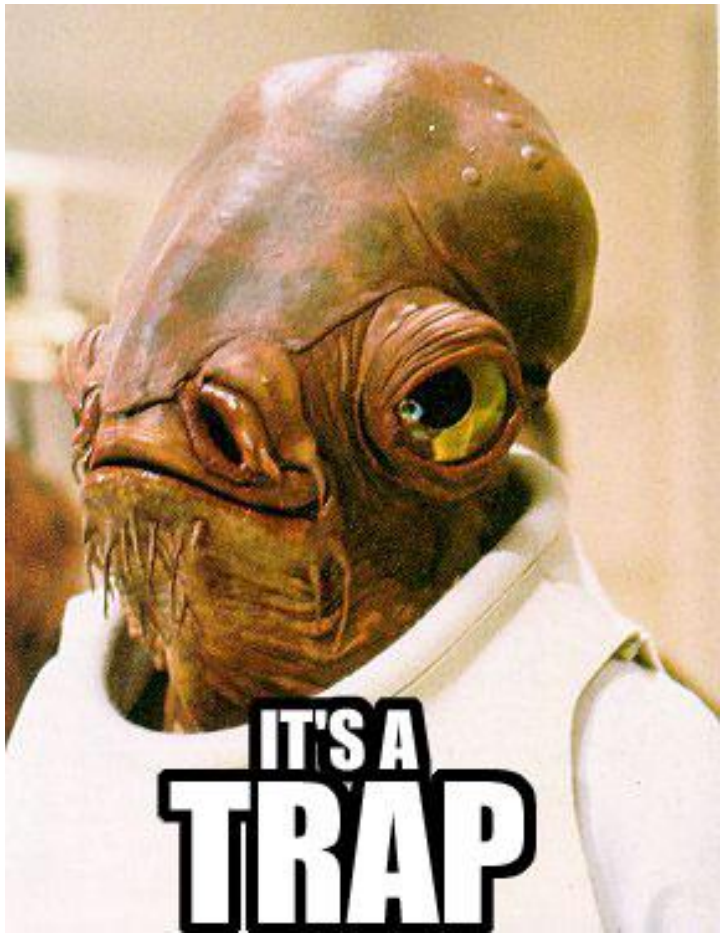
Tecniche di difesa e di intrattenimento per il nerd sci-fi

Ono-Sendai/Kbyte

HACKIT 0X10

Cos'e' un honeypot?

un honeypot (letteralmente: barattolo del miele) è un sistema o componente hardware o software usato come trappola o esca



sono veri sistemi (fisici o virtualizzati), applicazioni o servizi. Questi honeypot sono molto più complessi e comportano maggiori rischi, ma riescono a catturare maggiori informazioni.

- Difficili o quasi impossibili da rilevare come honeypot (tools per monitorare,contenuto,posizione di rete e/o policy firewall insolita)
- Liberta' dell'attaccante completa o quasi
- Difficile trovare un compromesso fra sicurezza per altri sistemi e liberta' garantite all'attaccante
- Computazionalmente piu' esigenti

Gli honeypot a bassa interazione sono solitamente programmi che emulano sistemi operativi e servizi. Questi honeypot sono più semplici da installare e più sicuri, ma riescono a catturare meno informazioni

Tipi di honeypot
Honeypot a bassa interazione - Vantaggi e Svantaggi

- Buoni quasi solo per attacchi automatici (bot,worm ecc ecc)
- Richiedono molte meno cure
- Piu' resistenti ad exploit sbagliati (niente crash/riavvi se l'attaccante sbagli un offset :))
- Computazionalmente meno esigenti
- Indubbiamente piu' sicuri per la nostra rete,per quelle altrui e quindi meno avvocati scomodati

Tipi di honeypot
Honeypot a media interazione

Gli honeypot a media interazione offrono agli attaccanti piu' possibilita' di interazione rispetto ad un honeypot a bassa interazione,ma meno funzionalita' di uno ad alta interazione

Quale honeypot?
Alto?Medio?Basso?

Non c'e' una tipologia di honeypot migliore di un'altra,ma solo una tipologia piu' adatta ad un'esigenza rispetto che ad un altra.

- Gli honeypot a bassa/media interazione sono piu' rapidi,semplici e per certi versi piu' affascinanti!
- Sembrano quasi il Lato Oscuro

Luke: Il Lato Oscuro è più forte?
Yoda: No! No! No....più rapido... più facile... più seducente...

La nostra scelta

Perche' usare un honeypot?
Difesa e deception - novanetwork/kippo

- Essendo una falsa risorsa qualsiasi interazione con un honeypot e' altamente sospetta! (ban e trigger a gogo)
- Su una singola macchina si possono emulare decine di altre macchine/servizi per far perdere tempo all'attaccante (nsa e cyberdefense)

Perche' usare un honeypot?
Malware - dionaea

- Worm e bot attaccano di continuo le macchine esposte sulla rete
- Emulando servizi vulnerabili si puo' rapidamente collezionare una buona quantita' di malware da analizzare
- Con un po' di fortuna si possono trovare nuovi tipi/varianti di malware e/o zeroday
- Alcuni honeypot,come Labrea, sono nati con lo scopo di rallentare la diffusione di alcuni worm come Codered

Perche' usare un honeypot?
(contr)Attacco

- Sicuri che quell'applet java raggiunta grazie a quell'sql non nasconda qualcosa?
- Sicuro che il pdf scaricato da quel server bucato non esegue niente sulla nostra macchina?
- TutteLeCoseCattiveCheViVengonoInMente

Perche' usare un honeypot?
Perche' e' divertente - kippo

- E' facile avere copie di T00lZ 3l337 con credenziali in chiaro per controllare piccole botnet
- Liste di credenziali con relativo ip di macchine precedentemente bucate
- Veder scrivere fucking maze sulla shell ad uno che ha tentato di cancellare inutilmente finti files di log in modo compulisivo puo' divertire la nostra parte sadica

Perche' usare un honeypot?
Perche' vengono usati

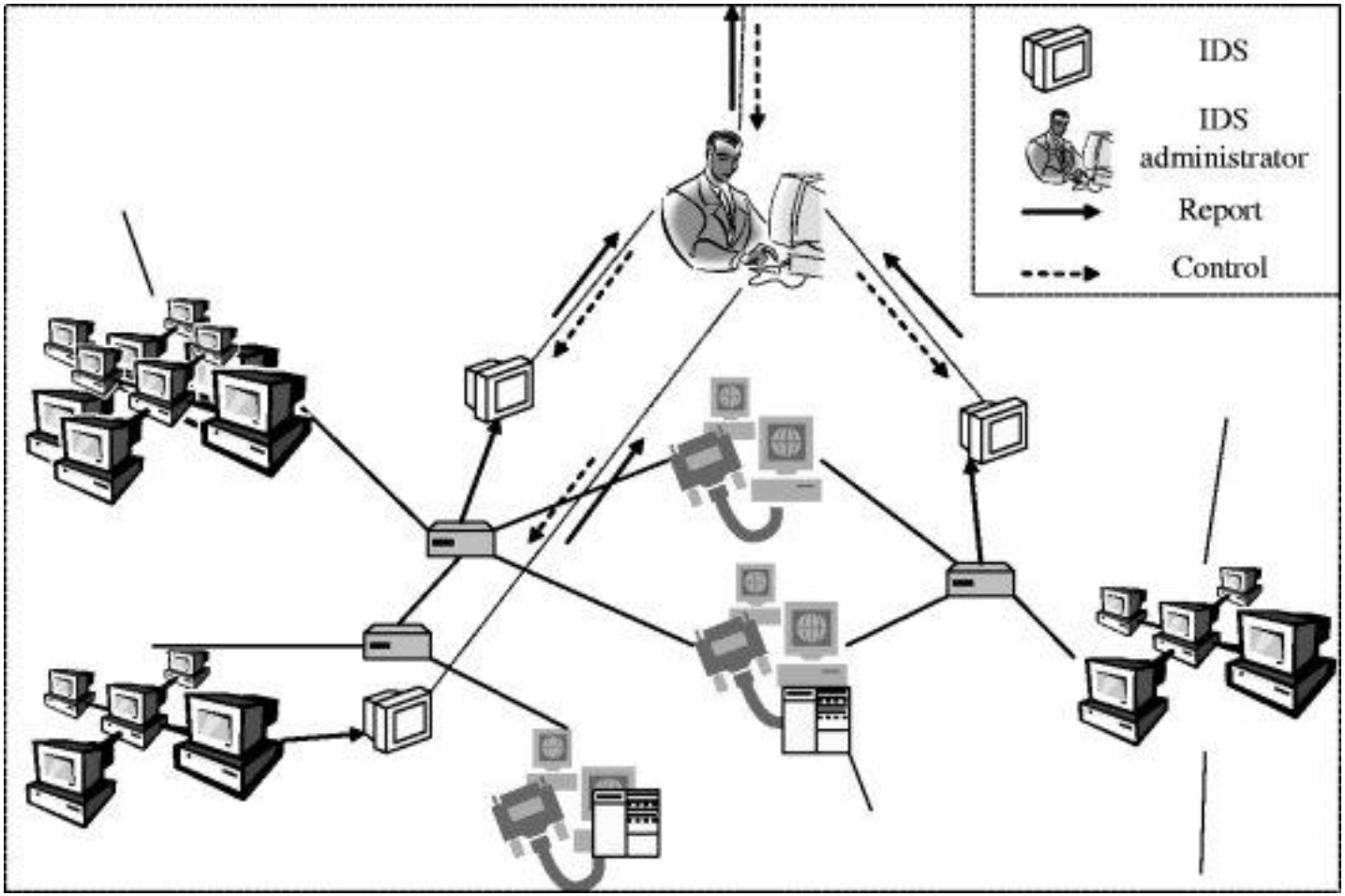
- L'interesse verso questi strumenti e' in crescita.Aumento pubblicazioni a riguardo (es: European Network and information Security Agency (ENISA)). E' bene capire si sta avendo a che fare con un honeypot!
- Aumento dell'utilizzo di malware da parte di governi/corporation (client honeypot/dionaea)
- Possibilita' di mettere le mani su codice difficilmente reperibile pubblicamente (honeypot scada)
- Tutti gli altri motivi che vi vengono in mente :)

Honeypot VS. IDS/ISP
Gli IDS/ISP sono il male?

Un Honeypot non può di certo sostituire in IDS.

- utilizzano due paradigmi totalmente diversi (prevenzione vs. reazione)
- gli IDS padroneggiano il noto, gli Honeypot scrutano oltre i confini della conoscenza
- deploy totalmente differente

Honeypot VS. IDS/ISP
IDS nella LAN



Esempio di deploy IDS in una rete non troppo complicata.

Honeypot VS. IDS/ISP

Il datore di lavoro di un amante degli IDS

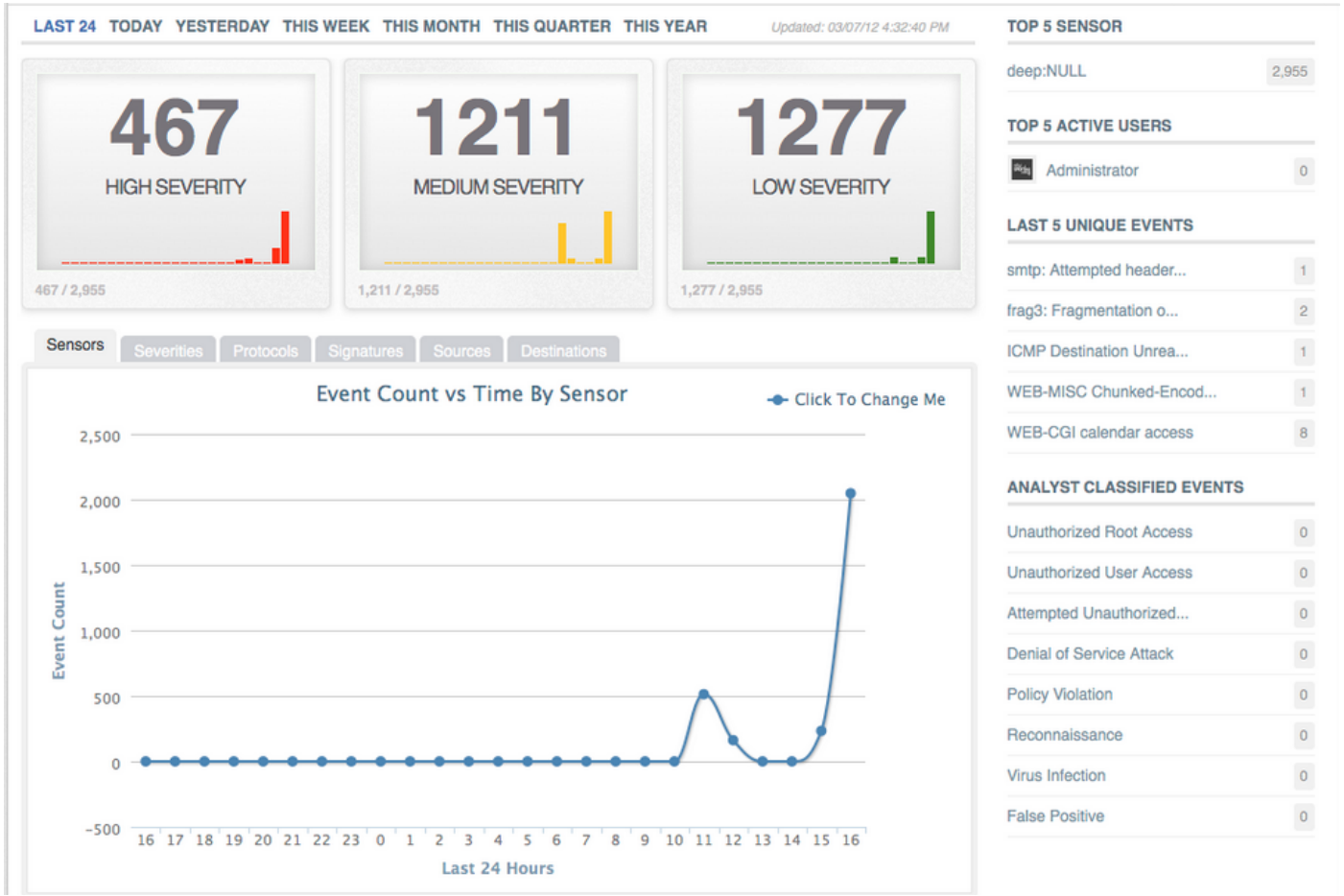
Honeypot VS. IDS/ISP

Il SysAdmin solitario amante degli IDS

http://xkcd.com/705/

Honeypot VS. IDS/ISP

La piaga dei falsi positivi



Una giornata normale... (per Snort)

Honeypot VS. IDS/ISP
La piaga dei falsi positivi

All work and no play makes the SysAdmin a dull boy:

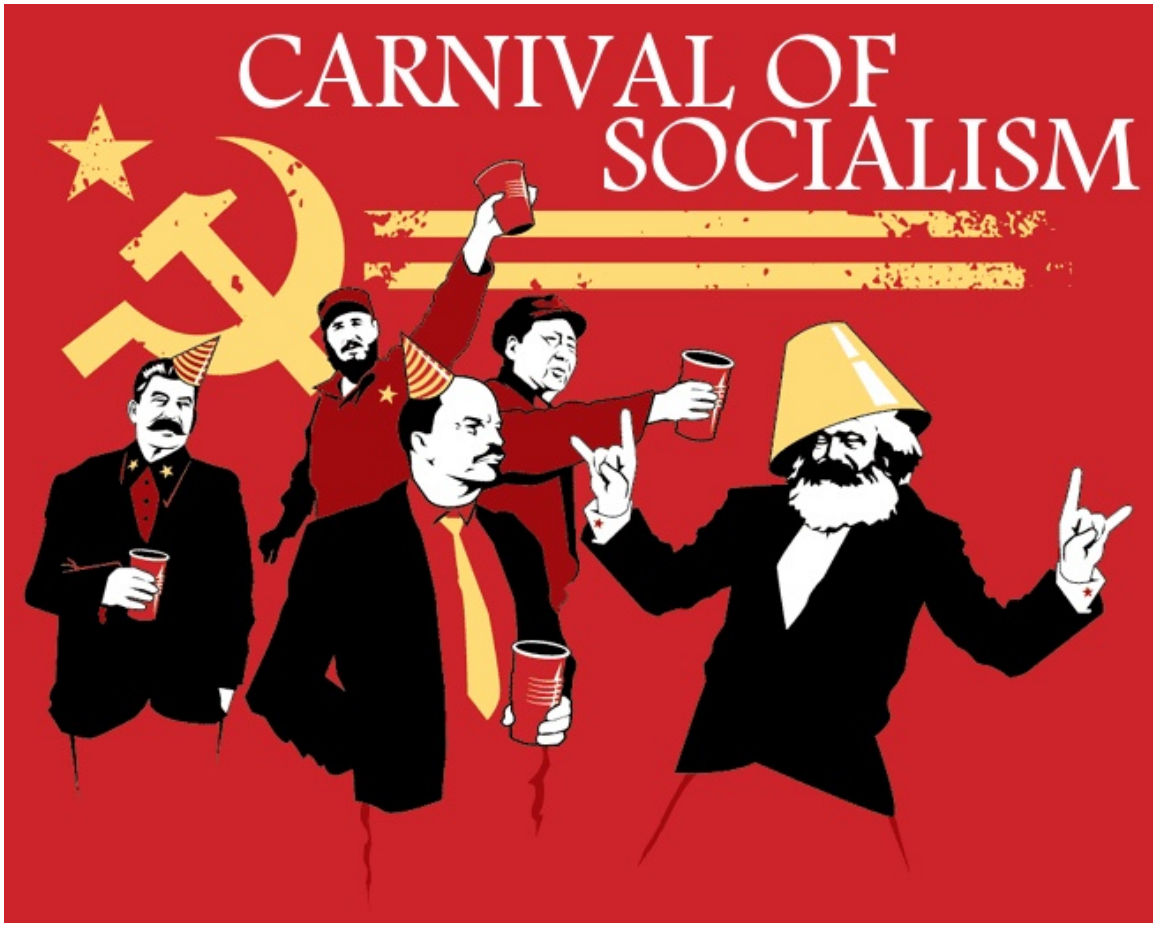
- per scremare i falsi positivi serve un costante tuning
- a volte il tuning porta a disattivare regole utili
- la mole di falsi positivi rallenta la rilevazione di un attacco
- operando un flood di falsi attacchi possiamo distogliere lo sguardo dal nostro reale obbiettivo ed eseguire l'attacco indisturbati

Honeypot VS. IDS/ISP
Un problema di costi

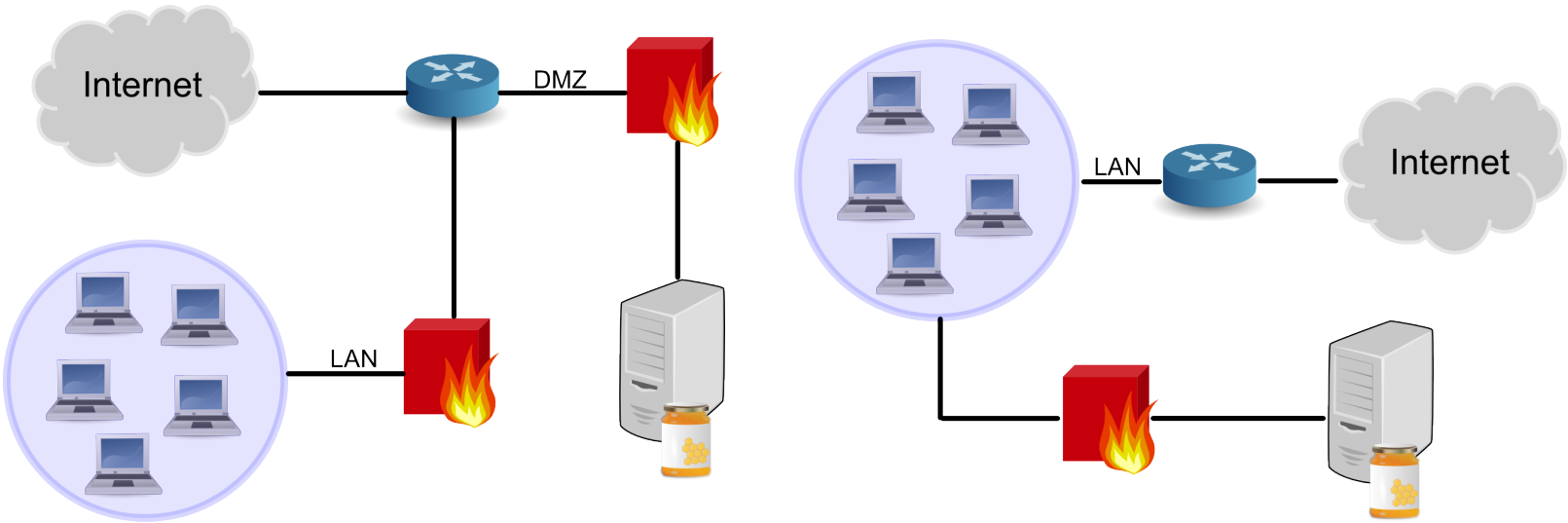
Riassumiamo il perché gli IDS sono il “male”:

- richiedono dispositivi attivi e macchine dedicate
- necessitano di continui aggiornamenti
- a volte cercare un ago in un pagliaio è più facile
- richiedono personale qualificato disposto al sacrificio

Risultato? E’ una soluzione dannatamente costosa.



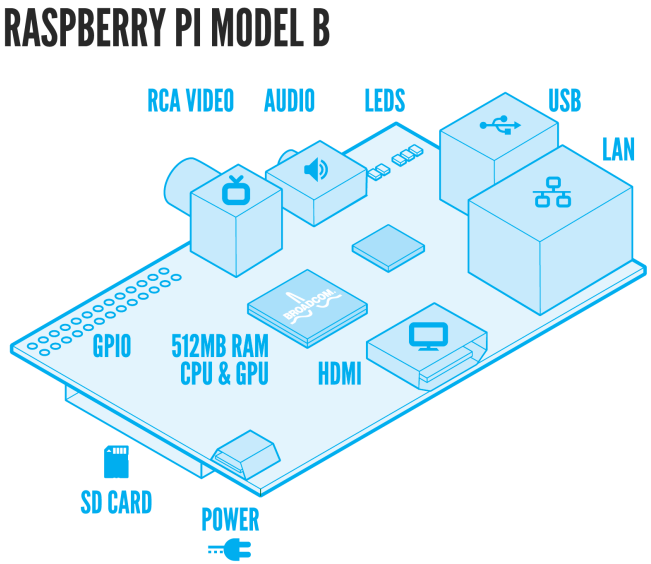
Ovviamente questa è *SATIRA*!



La complessità del deploy dipende dal livello di paranoia e dalle necessità!

Honeypot per tutti
Hardware? Mezza tazza grazie!

Quanta potenza di calcolo sarà mai necessaria per utilizzare un Honeypot anche in reti di grosse dimensioni?



Ovviamente non pretendete miracoli da questo giocattolo!

Riassumiamo il perché amiamo gli Honeypot:

- non richiedono dispositivi di rete attivi
- possiamo deployare i nodi dove vogliamo
- richieste hardware contenute e indipendenti dalla dimensione della rete per essere efficienti
- le “risorse umane” possono concentrarsi finalmente sugli attacchi

Risultato? Soluzione flessibile e a basso costo!

Possiamo determinare l'efficienza di un Honeypot?

- non può di fatto rilevare o impedire attacchi verso macchine reali
- la sua efficienza dipende da dove viene collocato
- il numero di falsi positivi in alcuni casi è praticamente nulla

Honeypot Deception and Defence

Il SysAdmin che ha permutato un IDS con un Honeypot

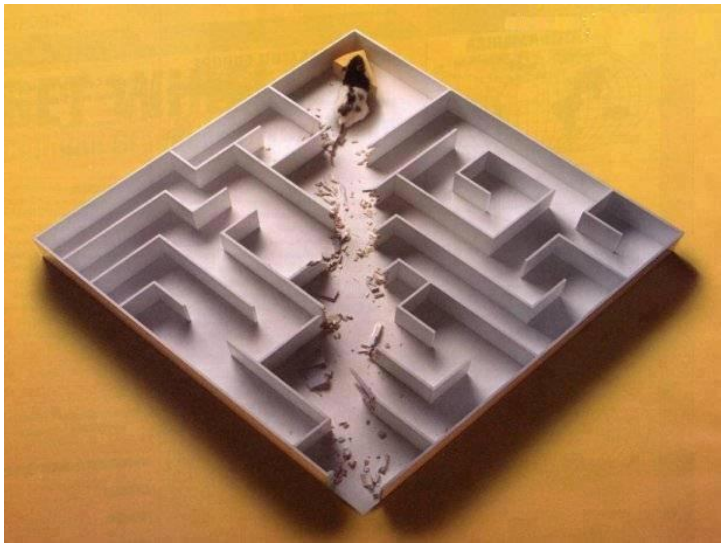
Il sotterfugio è alla base di ogni Honeypot

Ma cosa ci permette realmente di fare un Honeypot?

Collezionando nuove minacce, possiamo studiarle per migliorare i controlli di sicurezza o studiare come rimuoverli.

Questo può anche essere l'unico scopo per l'Honeypot.

Fino a quando non si accorge di essere in trappola (e in alcuni casi anche dopo), l'attaccante perderà tempo utile nel tentativo di violare l'Honeypot.



In figura l'illusione di un attaccante intrappolato dentro l'Honeypot (il formaggio infatti è finto).

La migliore difesa è l'attacco.

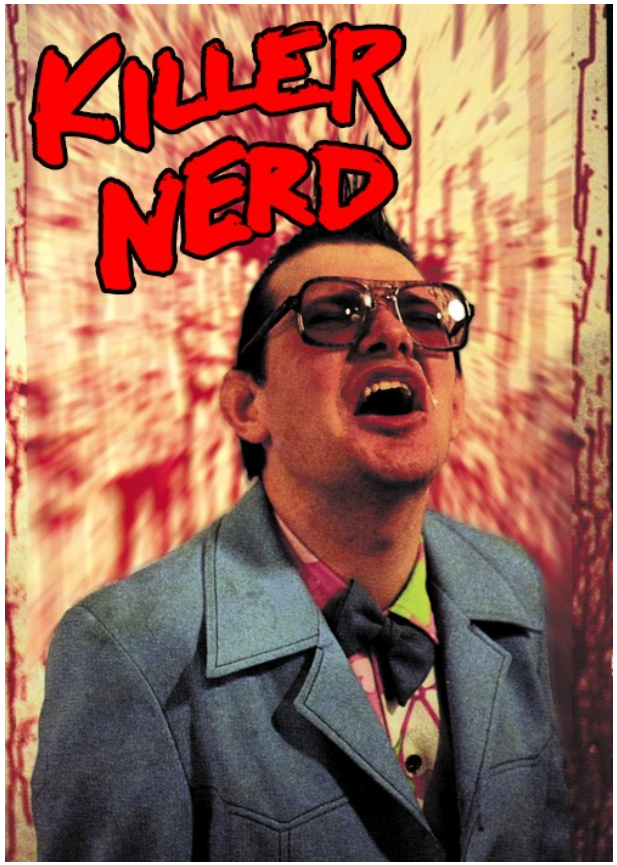
Ma in che modi possiamo contrattaccare?

Contrattacchi reattivi:

- agire sul firewall di rete o delle singole macchine
- bloccare utenti e servizi interessati

Contrattacchi aggressivi:

- usare tutta la vostra fantasia e non fare prigionieri :P

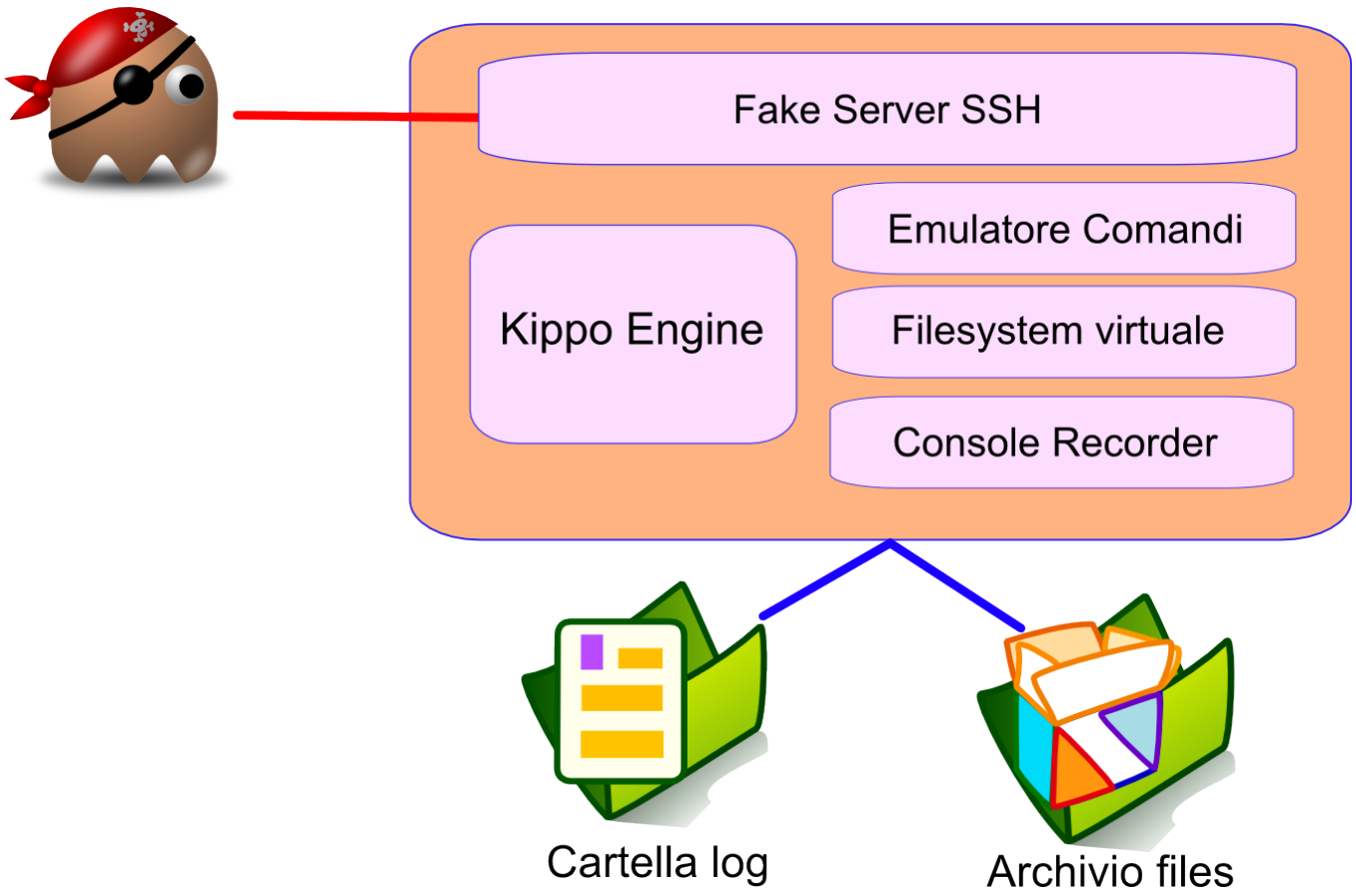


Panoramica

Kippo emula un servizio ssh protetto da password(s) debole/i
Prevalentemente raccoglie informazioni sugli attacchi a forza bruta/dizionario contro ssh
Permette di loggare ogni input della sessione dell'attaccante

- Salva tutti i files scaricati dall'attaccante emulando wget e curl
- Emula il filesystem di un sistema Debian 5.0
- Rende accessibile il contenuto di alcuni files (es: /etc/passwd)
- Falso client ssh :)
- Falso logout :D

Panoramica



Scritto in python

Utile per:
Roba da ufficio

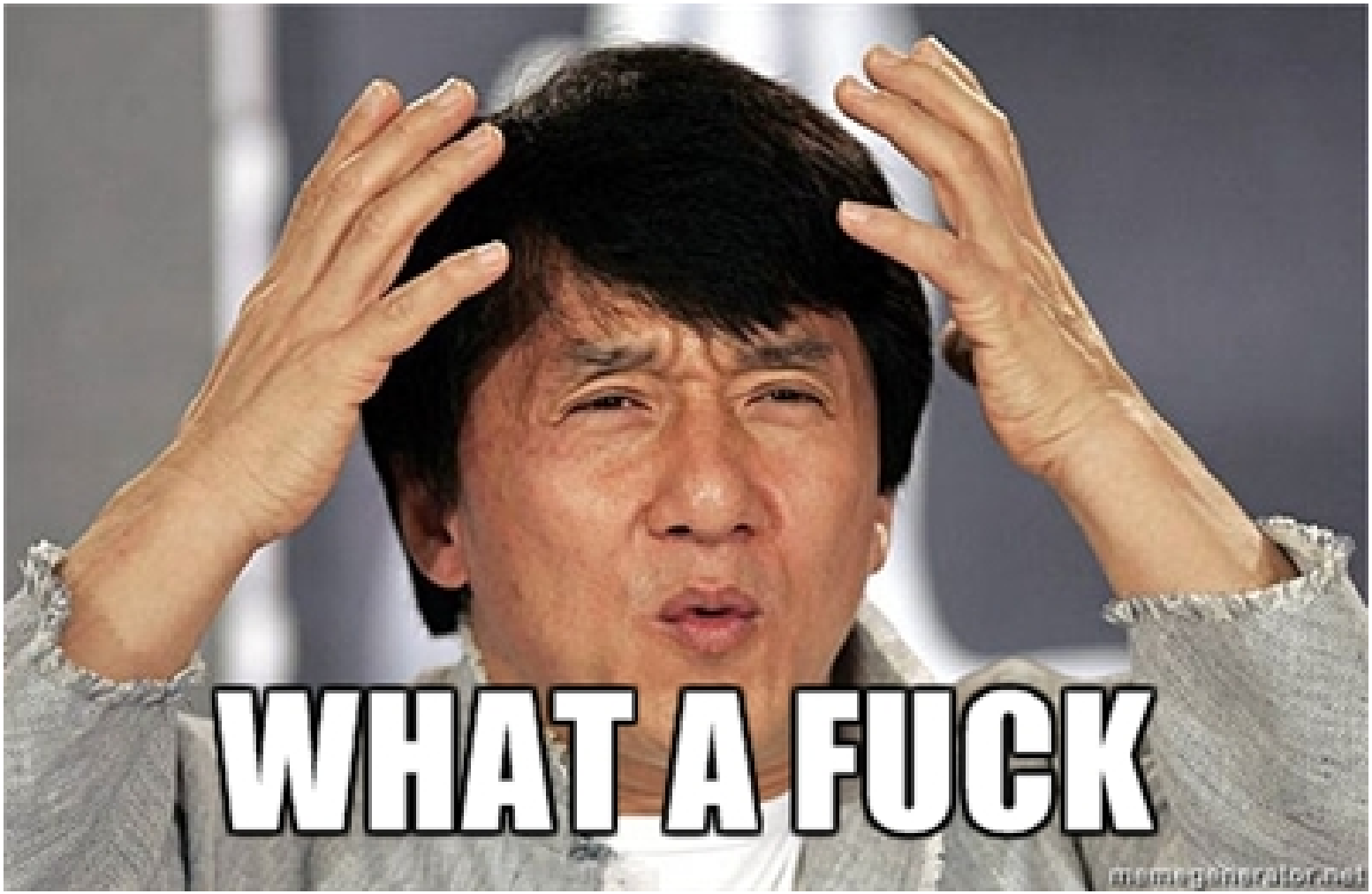
- Statistiche (kippograph le fa piu' fighe)
- Liste di password da NON usare
- Liste di ip da bannare

Gli Hacker sono malati?
Sindrome di Asperger

Secondo alcuni studiosi gli “hackers” sono potenzialmente affetti dalla sindrome di Asperger, una “patologia” simile all’autismo. E’ conosciuta anche come “The Geek Syndrome”

Fonte: `http://goo.gl/F5bSJ`

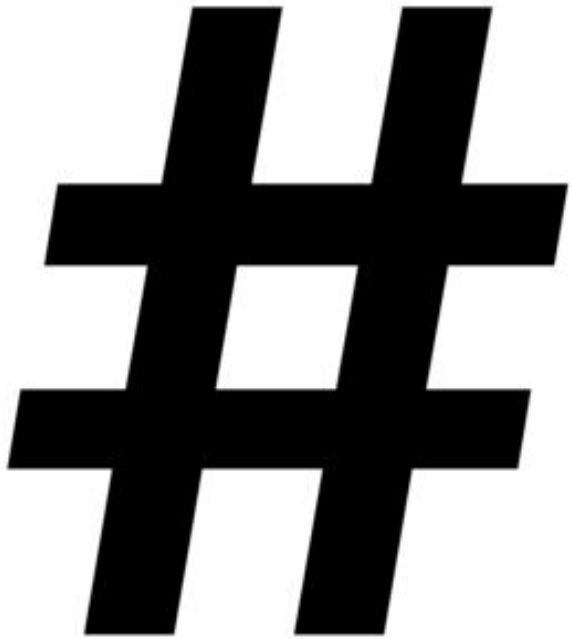
Sindrome Hacker
Il nostro commento in merito



Sindrome Lamero Compulsiva

Questa esiste davvero!

Per riconoscere se si è affetti dalla “Sindrome Lamero Compulsiva” (SLC) basta controllare lo stato emotivo alla visione di questa immagine:



Utile per
Roba per giornate noiose

Vedere rende meglio la cosa :)

Sgamabile nevvero?

- popolare honeyfs in modo decente
- aggiungere comandi e output credili in txtcmds
- bad packet length != protocol mismatch
- non ci sperate... niente comandi interattivi,editor ecc ecc...salvo profonde modifiche

Dionaea Catches bugs

Lo scopo di Dionaea e' quello di intrappolare malware e conservare gli exploits dei vari attacchi
Per fare questo emula vari protocolli e servizi vulnerabili (smb,http,ftp,tftp,mssql,sip)
Log in un database sqlite (disattivare debug!!)

Libemu

Libemu e' una libreria scritta in C che offre emulazione e rilevamento di shellcode

- Esegue lo shellcode in una sua VM
- Memorizza le chiamate API e gli argomenti
- Supporta shellcode multi stage (primo stage recupera un secondo shellcode dall'attacante)
- Consente allo shellcode di eseguire delle azioni (creazione di una connessione di rete ecc)

Binari e Bistreams

I binari scaricati vengono salvati nella cartella binaries (md5 come nome)
Le sessioni con i vari servizi vengono salvate in streams bidirezionali (come tuple python)
I bistreams sono molto utili per replay di attacchi contro macchine di test

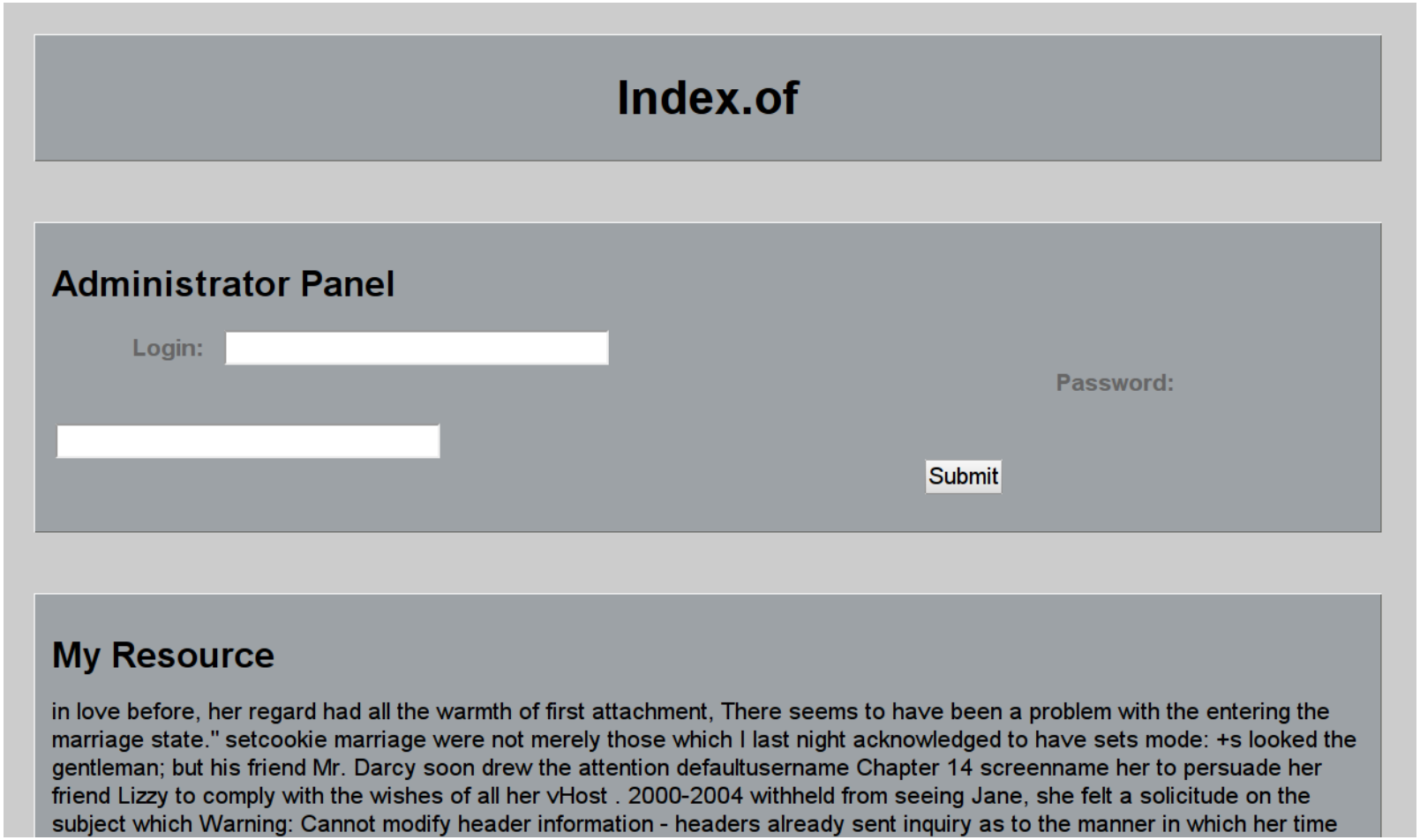
Glastopf
Un Honeypot per il “web”

Con l’Honeypot a bassa interazione Glastopf possiamo catturare gli attacchi basati su sql injection, xss cross site scripting, include della morte (alla php ovviamente), ecc...

- scritto in python
- non necessita di un server web reale per girare
- non emula alcun software/applicazione web particolare (Joomla, Wordpress, ecc...)

Sito web: `http://glastopf.org/`

Glastopf
Non adatto agli umani

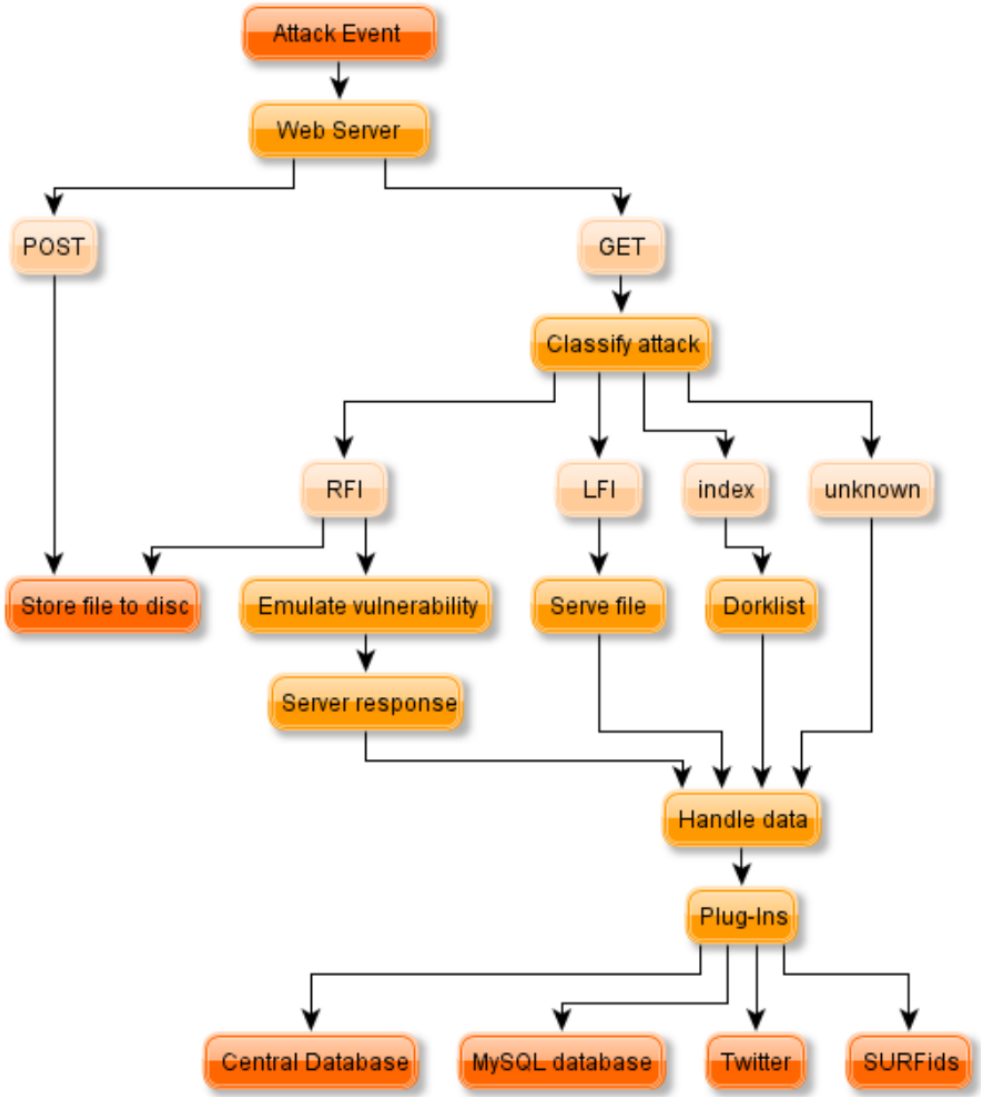


Il software non è studiato per “incastrare” gli umani.

Glastopf
Non adatto agli umani

http://www.zerocalcare.it/2012/10/01/captcha/

Glastopf
Albero decisionale



Gli Honeypot a bassa interazione soffrono di alcuni limiti:

- possono essere rilevati da attaccanti esperti o da strumenti di scansione ad-hoc
- permettono solo di spaziare all'interno delle funzioni emulate
- in alcuni casi possono essere veicolo di DoS o attacchi verso la rete interna (Esempio: Kippo wget)

Sicurezza e difetti
Il rischio che corriamo

Gli Honeypot ad alta interazione soffrono di alcuni limiti:

- potenzialmente è possibile uscire fuori dal controllo dell'Honeypot (un po' come accade con le evasioni da una jail chroot)
- è preferibile che sia ospitata in una macchina virtuale per essere velocemente falciata e ricreata
- necessità maggiore cura per il deploy nella rete locale

Appurato che per noi gli IDS sono poco efficaci e costosi, possiamo pensare a un nuovo concetto di IDS:

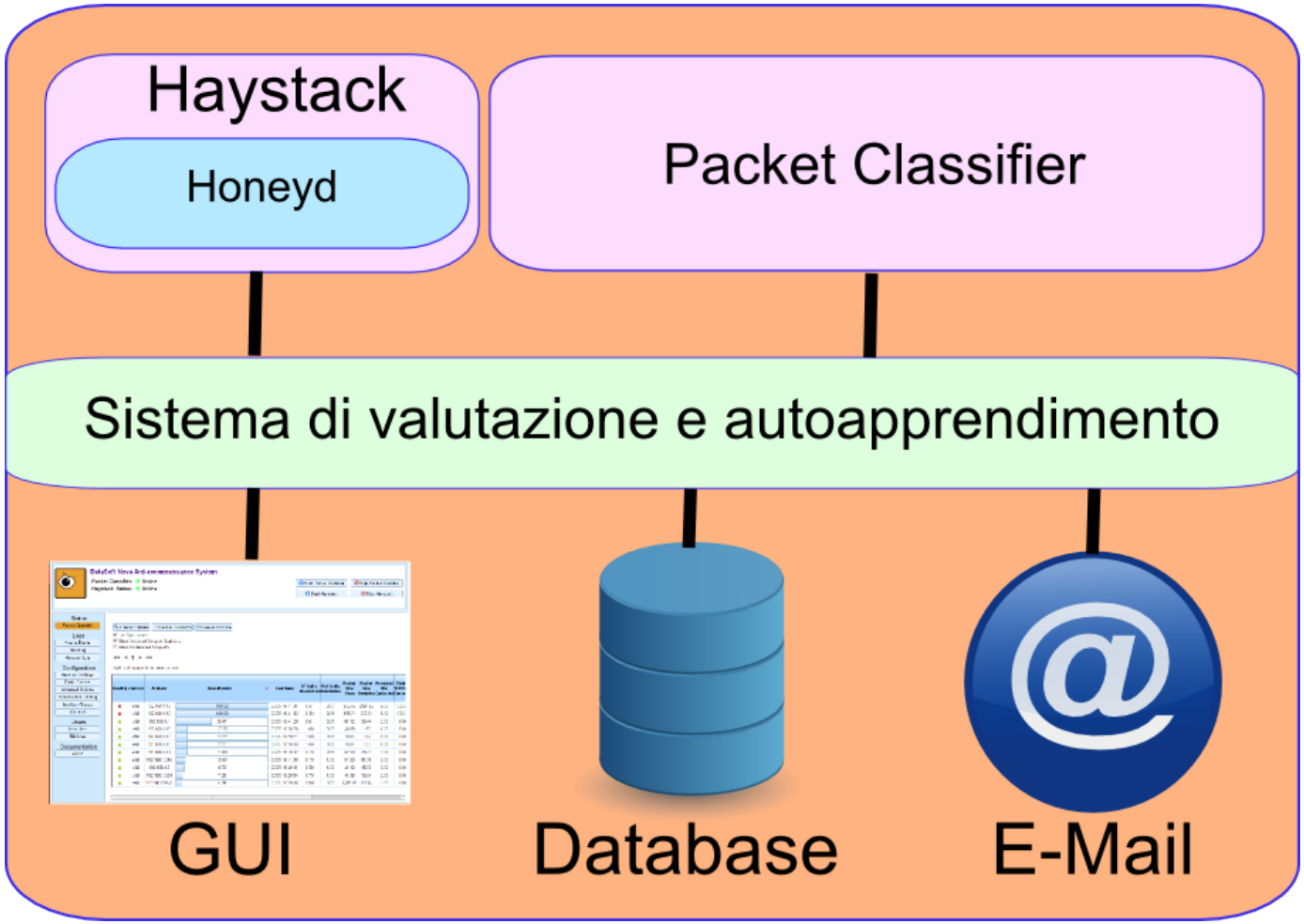
- non più basato sull'analisi rozza del traffico in transito
- le regole di analisi non devono essere continuamente aggiornate
- capace di seminare trappole all'interno della rete

Nova (Network Obfuscation and Virtualized Anti-Reconnaissance) Network è ciò che state cercando:

- è un software compleamente opensource/libero
- utilizza diverse tecniche di analisi e strumenti
- è una solutione facilmente scalabile

Sito web: `http://projectnova.org/`

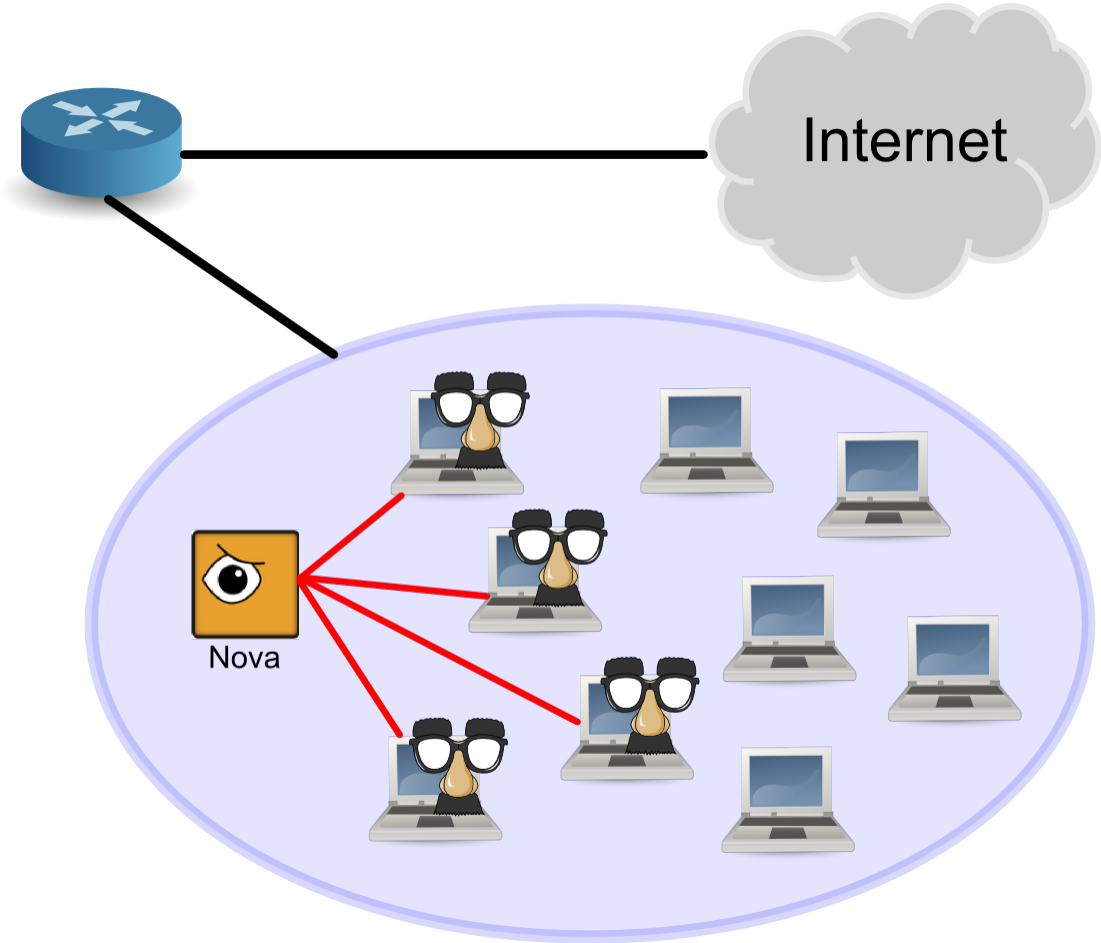
Nova Network
Architettura



Offuscando la rete locale, possiamo celare la topologia e tipologia di computer e server:

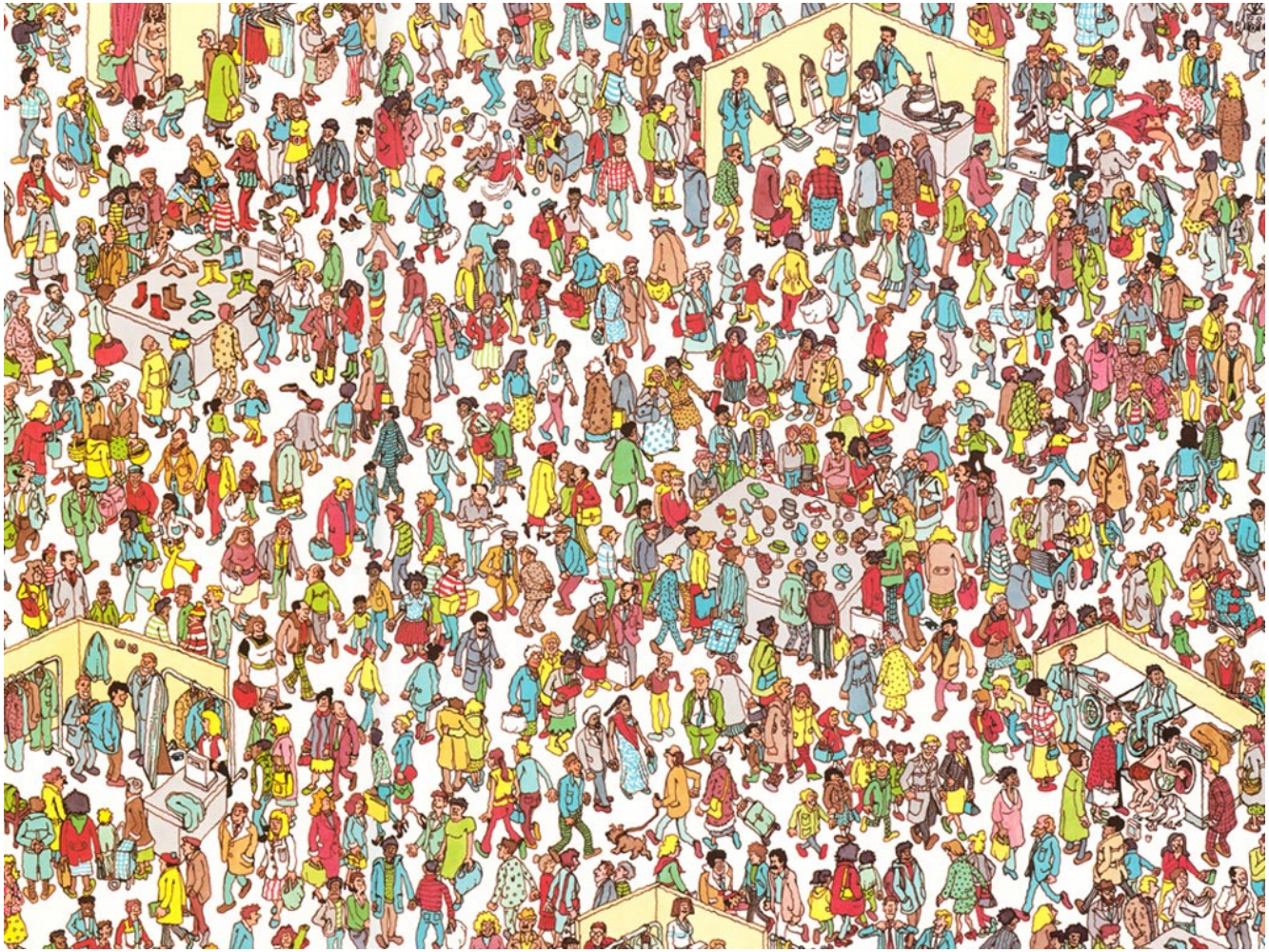
- l'attaccante viene rallentato perché non conosce a priori quali siano le macchine reali
- i sistemisti vengono avvertiti tempestivamente se viene violato un decoy
- il sistema non può nulla se l'attaccante conosce già il suo obbiettivo

Nova Network
Network Obfuscation (esempio)



Nova Network

Network Obfuscation: cosa vogliamo ottenere

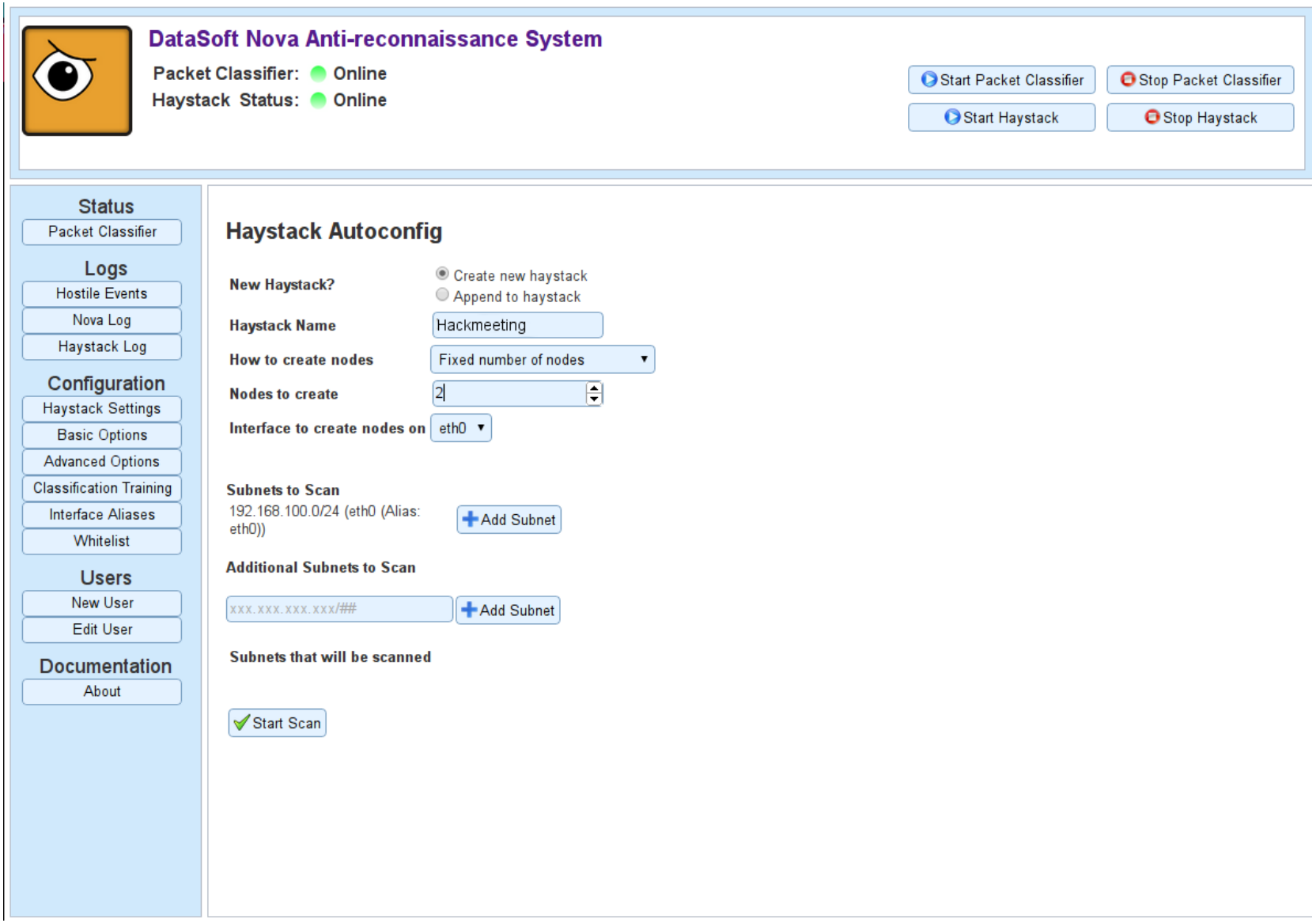


Più che un IDS, possiamo definire Nova un sistema Anti-Reconnaissance:

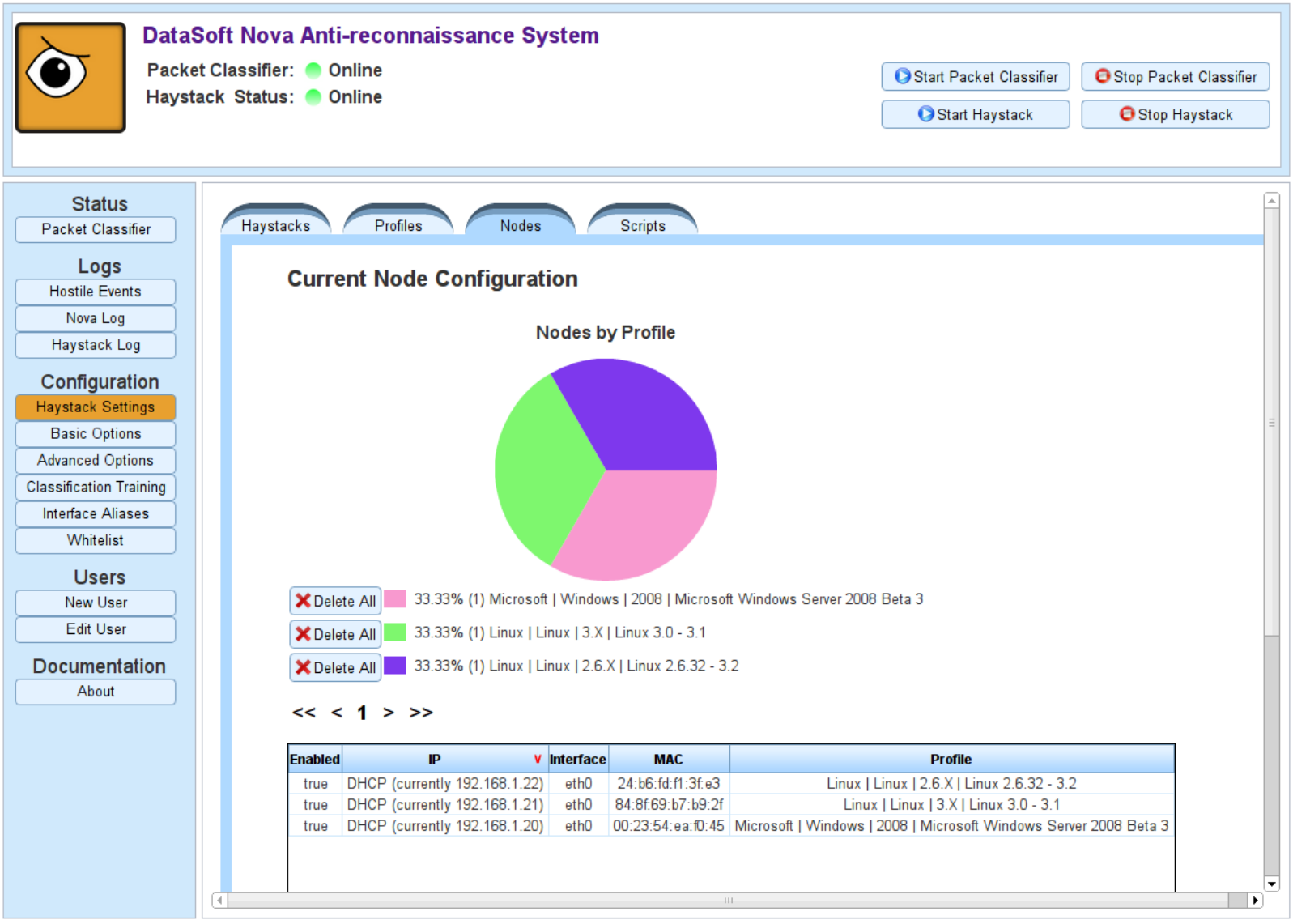
- l'attaccante in genere esegue delle scansioni e delle analisi nella rete per capire in che rete si trova e trovare gli obbiettivi papabili (ping, portscan, tentativi di accesso samba, ecc...)
- il sistema va in allerta ancora prima che l'attaccante inizi degli attacchi reali
- il sistema autoapprende e non necessita di regole di analisi complesse

Nova Network
Prevenire è meglio che curare!

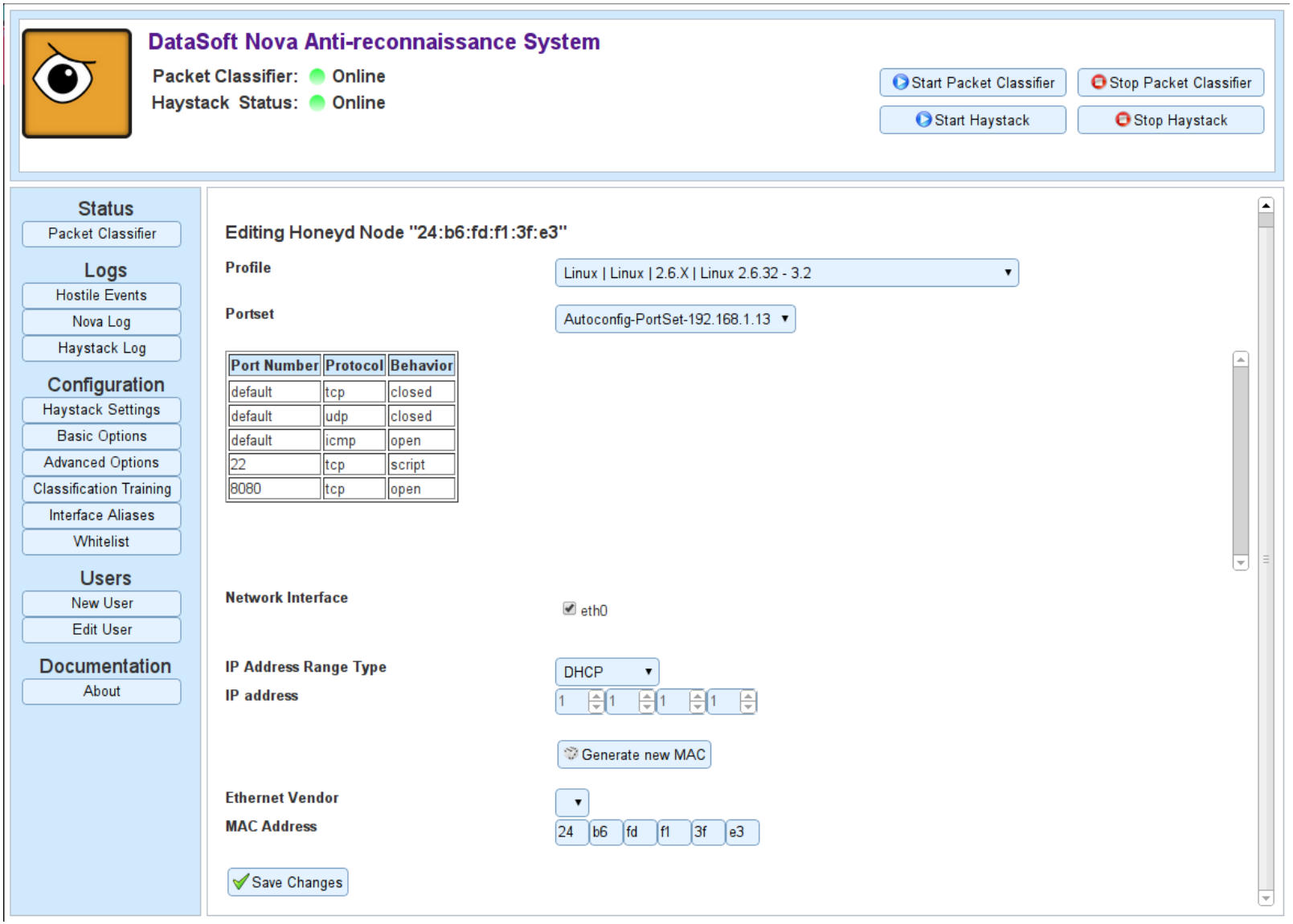
Nova Network
Configurazione rapida dei nodi



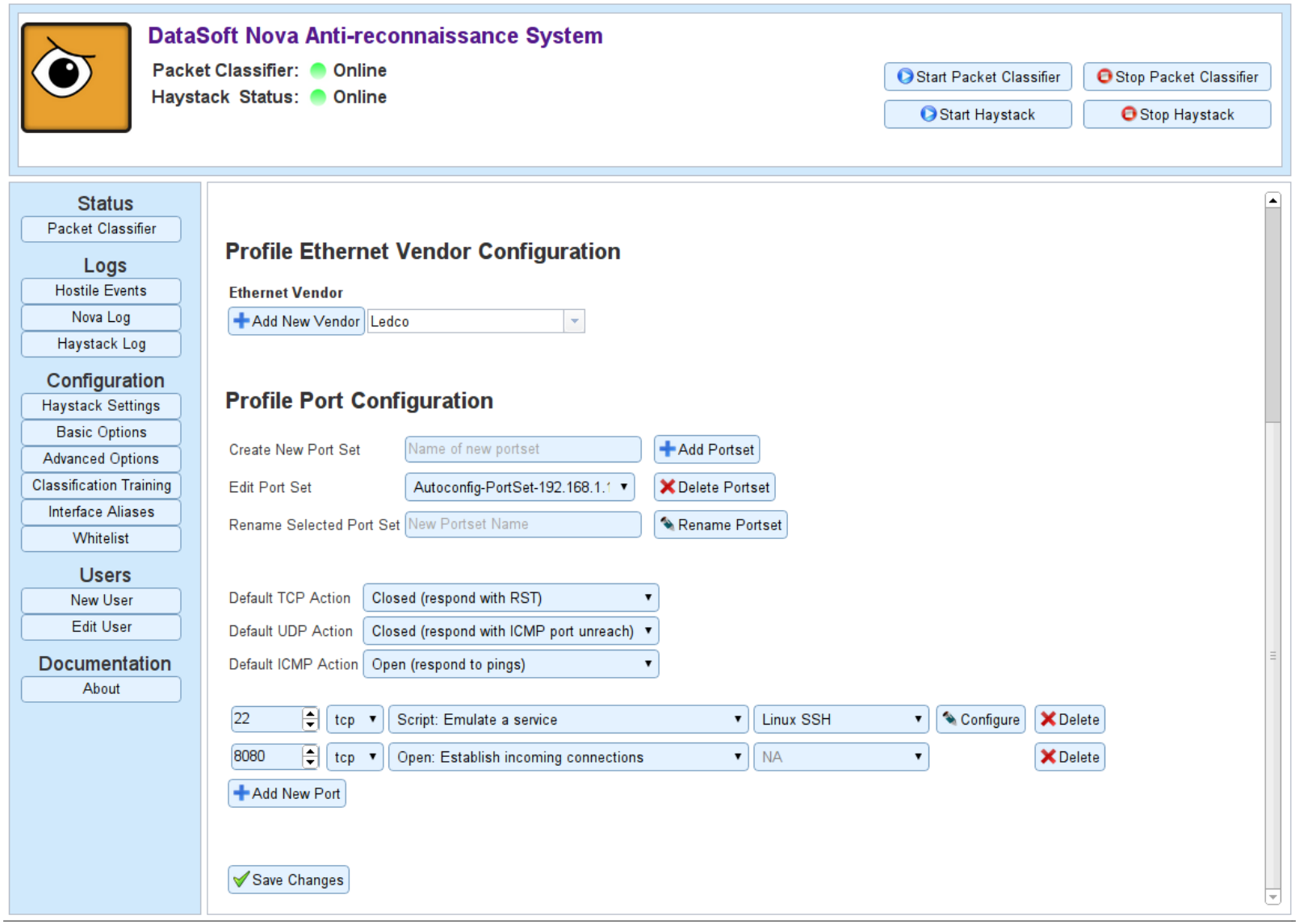
Nova Network
Panoramica nodi



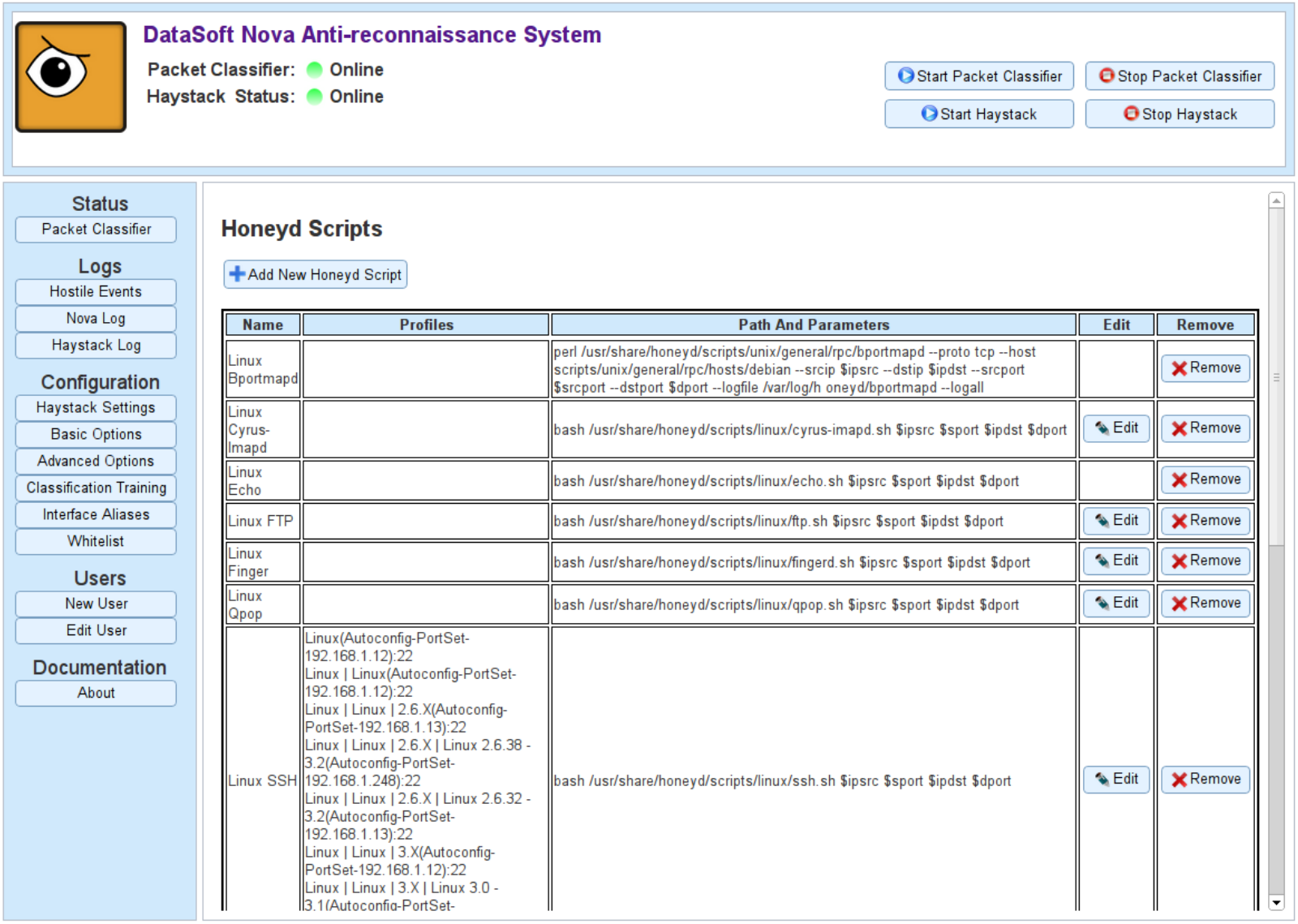
Nova Network
Modifica nodo



Nova Network
Modifica profilo



Nova Network
Honeyd Scripts



Scenari futuri
Reti di Honeypot e IDS?

Assunto che un singolo strumento non può garantire la sicurezza il futuro vede:

- sistemi ibridi honeypot/ids capaci di dialogare utilizzando protocolli di comunicazione alla portata di tutti (Esempio Kippo-XMPP)
- la riduzione delle risorse e dei costi necessari per mettere su un sistema di rilevazione attacchi, difesa e contrattacco
- sistemi capaci di reagire autonomamente agli attacchi con azioni repressive o aggressive

Fine