Snort – Network Intrusion Detection System

U Open Source svijetu Snort slovi za najbolji IDS alat, a to mjesto mu potvrđuje uporaba u mnogim komercijalnim i akademskim okolinama.

Kako dobiti najbolje od Snorta? Dali ga je u kombinaciji s Prelude-om moguće iskoristiti za cjelovito OS rješenje za nadzor sigurnosti velike mreže? Kakva su iskustva predavača u pokušaju implementacije takvog rješenja?

Božo Juretić <bjuretic@ouroboros.hr>

http://www.ouroboros.hr

ouroboros

CLUC/DORS 2004

Snort Network Intrusion Detection System

Snort – The Open Source Network Intrusion Detection System

- Najpopularniji Open Source IDS
- Dostupan od 1998. godine, još uvijek se razvija i nadopunjuje korisnim proširenjima funkcionalnosti (zadnja verzija 2.1.2)
- Glavni programer Martin Roesch osnovao firmu Sourcefire 2001. godine
- Velika i kvalitetna razvojna baza, pogotovo zbog interesa Sourcefire-a (komercijalna firma koja razvija Intrusion Detection softver baziran na dorađenoj Snort tehnologiji; poznati i po kontribuciji IDMEF specifikaciji)

Snort Network Intrusion Detection System

Popularnost Snorta

- Open Source (GPL)
- Kvalitetan i dobro održavan izvorni kod
- Multi-platformsko izvršavanje
- Dostupan u obliku prekonfiguriranih programskih paketa
- Dobra Open Source i komercijalna podrška
- Lako povezivanje s vanjskim aplikacijama (XML i binarni formati) za analizu napada te eventualno protuakciju
- Jednostavno dodavanje definicija napada (Snort rules)
- Dobra osnova za cjelovita sigurnosna rješenja (Open Source – Prelude, komercijalna - npr. Sourcefire rješnja) za nadzor sigurnosnog stanja mreže i eventualnu reakciju na napade

Primjena u svijetu i kod nas

- U OS zajednici *de facto* standard na području IDS tehnologije - “referentni IDS”
- Snort definicije napada su također referenca za ostale definicije tog tipa – konverzija Snort pravila u native format
- U komercijalnom svijetu rijetko primarni IDS (upotreba je uglavnom eksperimentalna), ali vjerojatno najkorišteniji *sekundarni* IDS na svijetu, bez obzira na domenu uporabe
- Nekoliko komercijalnih proizvođača bazira svoje sigurnosne proizvode na Snort tehnologiji
- Standardna uporaba u akademskoj (istraživačkoj) zajednici
  - npr. testiranja na SRCu za CARNet

Podrška

- Osim komercijalne podrške, “white hats” grupacije s community portalima
  - Whitehats Network Security Resource http://www.whitehats.com
    - Izdavanje alternativnih definicija napada
- Rješavanje problema preko distribucijskih listi, forumi
- Podrška u sklopu većih distribucija OS operacijskih sustava

Važnost dobrih definicija napada i konfiguracije – loše podešavanje

Vrsta napada	Broj napada
ICMP PING CyberKit 2.2 Windows	65722
ICMP PING NMAP	7908
ICMP Destination Unreachable (Communication Adm. Prohibited)	6706
WEB-MISC robots.txt access	6246
SCAN SOCKS Proxy attempt	228
WEB-FRONTPAGE /_vti_bin/ access	220
WEB-CGI formmail access	194
SCAN Proxy (8080) attempt	152
SCAN Squid Proxy attempt	148
WEB-CGI formmail arbitrary command exec attempt	98
ICMP Large ICMP Packet	86
WEB-MISC /doc/ access	68
WEB-MISC login.htm access	62
WEB-IIS view source via translate header	56
WEB-IIS cmd.exe access	45
WEB-CGI scriptalias access	43
ICMP Source Quench	34
SMTP rcpt to sed command attempt	27
SCAN nmap TCP	22
DNS zone transfer TCP	18

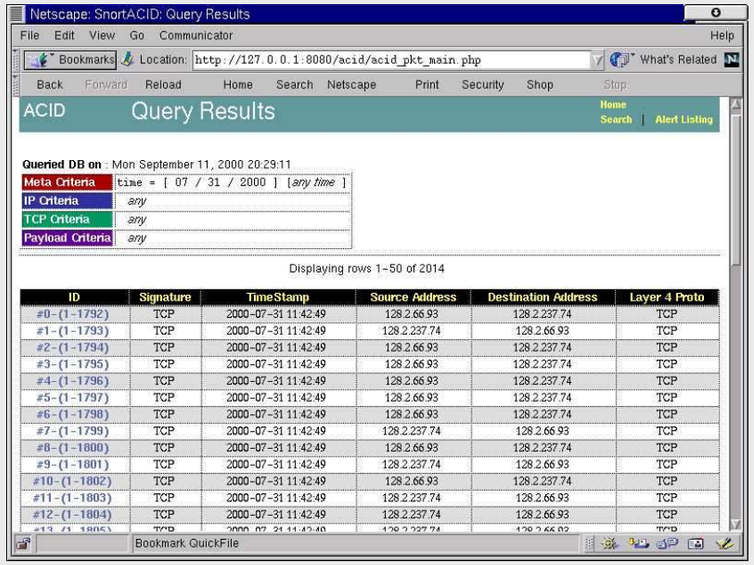
Snort Network Intrusion Detection System

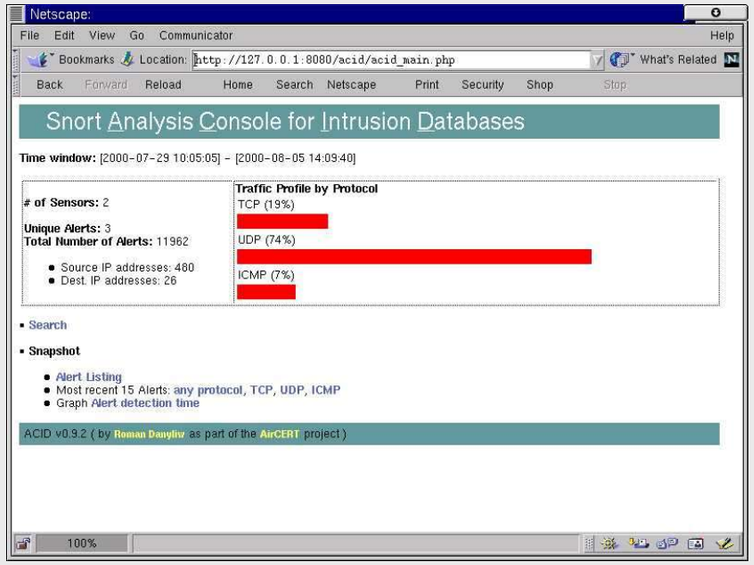
Važnost dobrih definicija napada i podešavanja Snorta

- Dobre definicije su osnova praktične iskoristivosti Snorta
- Proširenje definicijskog jezika pomoću sp_perl dodatka za kompleksne definicije napada u Perlu (potreban patch)
- Održavane definicije napada dostupne
  - http://www.whitehats.com/ids/
- Osim kvalitetnih definicija napada bitno je namjestiti dobre threshold vrijednosti (za napade koji se učestalo ponavljaju neće se slati obavijesti ukoliko ne prelaze određenu učestalost ponavljanja)

ACID – Analyst Console for Intrusion Databases

- Zgodno sučelje ali ne zadovoljava potrebe velikih mreža
- Rudimentarno
- Nije napravljeno kao višekorisničko sučelje
- Ipak upotrebljivo





Snort Network Intrusion Detection System

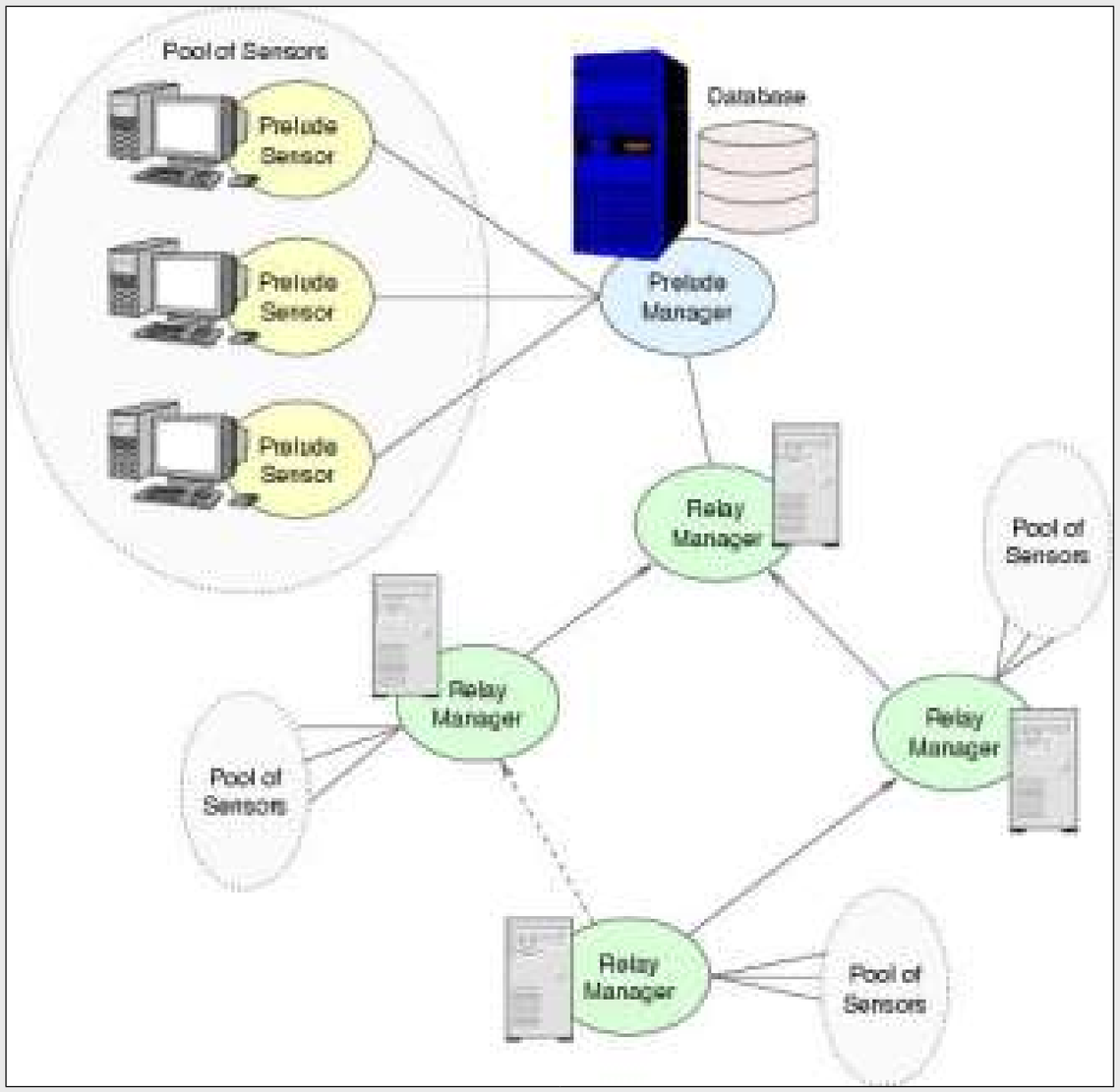
Prelude - cjelovite Open Source rješenje za osiguranje mreže

http://www.prelude-ids.org

- Prelude – Hybrid IDS
- Modularnost (Libprelude, Libsafe, Prelude LML, Prelude NIDS)
- Multi-platformska orijentacija, dostupni binarni RPM i Debian programski paketi
- Snort kao senzor (uz Prelude output plugin)
- Planirano povezivanje s AIDE-om (zanimljivost: AIDE ARMS na SRCu/CARNetu)
- Planirana reakcija na napade pomoću “agenata”
- Planovi za gigabitnu implementaciju

Snort Network Intrusion Detection System

Prelude Hybrid IDS arhitektura – distribuirana sigurnosna mreža



Prelude Manager sučelje

- Ostvareno je pomoću Piwi web sučelja (Perl) koji čita podatke iz Prelude baze sigurnosnih uzbuna

- Najčešći napadi
- Najčešći napadači
- Sortiranje po kategorijama (query builder)
- Filteri
- Heartbeat (pregled senzora u sustavu)
- Statistički izvještaji s grafovima

Prelude u praksi

- Komplicirana instalacija, pogotovo ako se ide na automatiziranu varijantu (nužno za veće instalacije)
- Piwi sučelje je sporo i nefunkcionalno
- Nedostatak podrške za više korisnika (posebno zanimljivo u mrežama gdje nema centralnog mjesta nadzora)
- Prelude datamodel je “školski implementiran” (doslovno po IDMEF specifikaciji)
  - Suboptimalno pristupanje podacima rezultira izrazitom sporošću odziva za sve osim najelementarnijih upita prema bazi
- Nedovršenost bitnih modula u kombinaciji s velikim ambicijama, malim razvojnim timom i nedostatkom izvora financiranja

Implementacija Prelude rješenja, da ili ne

- Uz sve nedostatke Prelude OS rješenje je obećavajuće
- Trenutno vjerojatno jedini kandidat koji nudi realnu mogućnost implementacije na velikim mrežama u dogledno vrijeme
- Bez kvalitetnih definicija napada, rješenje bazirano na Snortu nije upotrebljivo ni na malim ni velikim mrežama
- Prelude je potrebno iz “školske” dovesti u produkcijsku faze – ispravak datamodela i jednostavnije prijavljivanje novih senzora u Prelude mrežu, za početak
- Nužno je napisati kvalitetnije sučelje za pristup podacima

- ZAKLJUČAK:

  Potrebno je uložiti sredstva u razvoj Preludea i vjerojatno barem djelomično komercijalizirati projekt (Snort/Sourcefire model), što bi moglo uroditi prvim ozbiljnim cjelovitim OS rješenjem za nadzor sigurnosti mreže

Zahvale

- CARNet – Hrvatska akademska i istraživačka mreža

CARNet

- SRCE – Sveučilišni računski centar

srce
Sveučilište u Zagrebu
Sveučilišni računski centar