IDPS

Rilevamento e prevenzione intrusioni

19/01/2018

Concetti generali

Intrusione = attività pericolosa o contraria alle regole

Rilevamento intrusione -> invio allarme

Prevenzione -> interrompo traffico (+allarme)

Firme o anomalie (rkhunter / Bro)

HIDS e NIDS

Architettura di rete (span port / firewall)

Scenari: rete di pc, server interni, applicazioni, etc

NethSecurity

IDPS sul FireWall (FW)

Firme raggruppate in categorie

Analisi di tutto il traffico del FW (LAN->WAN, WAN->LAN, FW->WAN, WAN->FW)

NFQUEUE con bypass automatico

Storico alert con gestione “tipo inbox”

Software: Suricata - PulledPork - EveBox

Firme (regole)

Come un Antivirus su pkt invece di file (falsi allarmi)

Circa 15 mila regole (firme) divise in 40 categorie

Aggiornate una volta al giorno

Emerging threats

Fonti extra - Regole custom

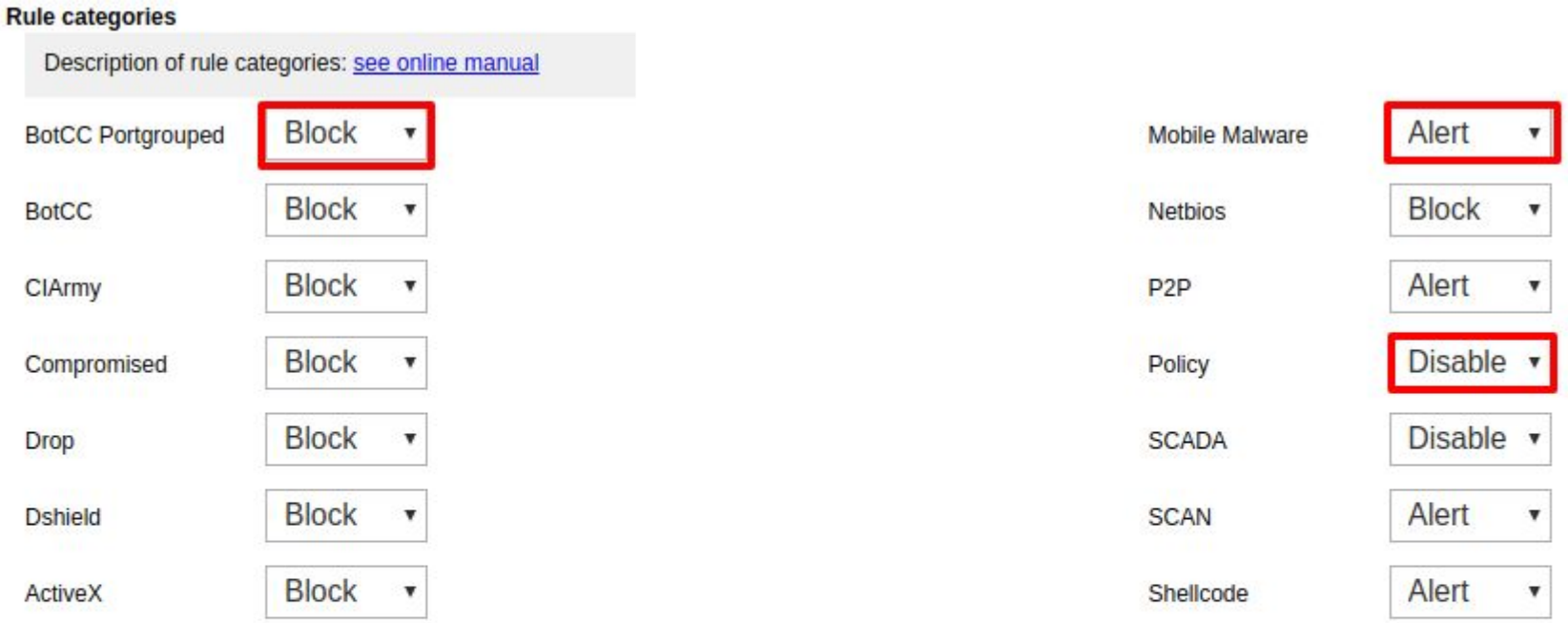
Vedere il manuale per una descrizione delle categorie

Categorie

ET-emerging-trojan.rules 5039
ET-emerging-web_specific_apps.rules 4021
ET-emerging-current_events.rules 2055
ET-emerging-malware.rules 984
ET-emerging-info.rules 460
ET-emerging-exploit.rules 447
ET-emerging-web_server.rules 419
ET-emerging-policy.rules 409
ET-emerging-activex.rules 409
ET-botcc.rules 245
ET-emerging-user_agents.rules 237
ET-emerging-web_client.rules 221
ET-emerging-mobile_malware.rules 194
ET-botcc.portgrouped.rules 187
ET-emerging-scan.rules 172
ET-emerging-attack_response.rules 135
ET-ciarmy.rules 100
ET-emerging-dos.rules 61
ET-emerging-dns.rules 52
ET-emerging-p2p.rules 49

ET-emerging-shellcode.rules 48
ET-emerging-netbios.rules 47
ET-emerging-deleted.rules 47
ET-compromised.rules 40
ET-drop.rules 32
ET-emerging-scada.rules 15
ET-emerging-voip.rules 11
ET-emerging-worm.rules 10
ET-emerging-ftp.rules 10
ET-emerging-games.rules 9
ET-emerging-snmp.rules 8
ET-emerging-smtp.rules 8
ET-emerging-chat.rules 8
ET-emerging-tftp.rules 7
ET-emerging-telnet.rules 5
ET-emerging-sql.rules 1
ET-dshield.rules 1
ET-tor.rules 0
ET-emerging-misc.rules 0
ET-emerging-inappropriate.rules 0

Interfaccia



Esperienza diretta

Block sicuro:

- ET-botcc.portgrouped
- ET-botcc
- ET-ciarmy
- ET-compromised
- ET-drop
- ET-dshield

Block nella maggior parte delle reti:

- ET-emerging-activex
- ET-emerging-attack_response
- ET-emerging-dos
- ET-emerging-exploit
- ET-emerging-malware
- ET-emerging-netbios

Alert:

- Categorie rimanenti

Pulledpork

Ogni notte scarica le firme

Premendo SALVA da interfaccia applica la configurazione

Ricarica le regole in Suricata

/var/log/sid_changes.log

/var/log/suricata/suricata.log

```
18/1/2018 -- 02:32:21 - <Notice> - rule reload starting
18/1/2018 -- 02:32:25 - <Notice> - rule reload complete
```

Suricata

Analisi pacchetti:

IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE

Protocolli:

HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP/CIP, DNP3, NFS, NTP

Suricata - Prestazioni

Analisi del traffico richiede CPU

Taglio banda massima proporzionale alla potenza della CPU

Numero di regole attive influenza parzialmente le prestazioni

Nessuna regola o tutte le regole cambia “poco”

Esempio S150: Max banda = 1 Gbit

Esempio S20: Max banda = 150 Mbit (HTTP ~ 100 Mbit)

EveBox

Stile Inbox

Alerts

Events

Link al sito con note e storico regola. Esempio:

http://doc.emergingthreats.net/2018908

EveBox | Inbox | Escalated | Alerts | Events | Last week | Help | 0

Refresh | Select All | Filter... | Apply | Clear

Showing 1-100 of 305.

Newest | Newer | Older | Oldest

	#	Timestamp	Source/Dest	Signature	
☆	2520	2017-09-23 10:59:35 a few seconds ago	**S:** 148.251.243.162 **D:** 192.168.5.87	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	Archive
☆	53	2017-09-23 10:48:11 12 minutes ago	**S:** 208.67.220.220 **D:** 93.57.48.68	BLOCKED ET TROJAN Win32.Zbot.chas/Unruy.H Covert DNS CnC Channel TXT Response	Archive
☆	3	2017-09-23 09:33:55 an hour ago	**S:** 139.60.160.135 **D:** 192.168.5.152	ET SCAN MS Terminal Server Traffic on Non-standard Port	Archive
☆	3	2017-09-23 09:05:07 2 hours ago	**S:** 80.82.70.133 **D:** 192.168.5.252	BLOCKED ET DROP Dshield Block Listed Source group 1	Archive
☆	2	2017-09-23 09:05:07 2 hours ago	**S:** 80.82.70.133 **D:** 192.168.5.252	BLOCKED ET CINS Active Threat Intelligence Poor Reputation IP group 47	Archive
☆	9	2017-09-23 08:12:37 3 hours ago	**S:** 46.174.191.28 **D:** 192.168.5.150	BLOCKED ET CINS Active Threat Intelligence Poor Reputation IP group 21	Archive
☆	1	2017-09-23 08:02:57 3 hours ago	**S:** 141.212.122.92 **D:** 192.168.5.252	BLOCKED ET DROP Dshield Block Listed Source group 1	Archive
☆	3	2017-09-23 07:19:54 4 hours ago	**S:** 159.203.244.106 **D:** 192.168.5.252	BLOCKED ET DROP Dshield Block Listed Source group 1	Archive
☆	1	2017-09-23 06:24:53 5 hours ago	**S:** 104.236.178.199 **D:** 192.168.5.252	BLOCKED ET CINS Active Threat Intelligence Poor Reputation IP group 70	Archive
☆	1	2017-09-23 06:05:57 5 hours ago	**S:** 196.52.43.66 **D:** 93.57.48.68	BLOCKED ET DROP Dshield Block Listed Source group 1	Archive

Evento

Link in alto a destra [ET]

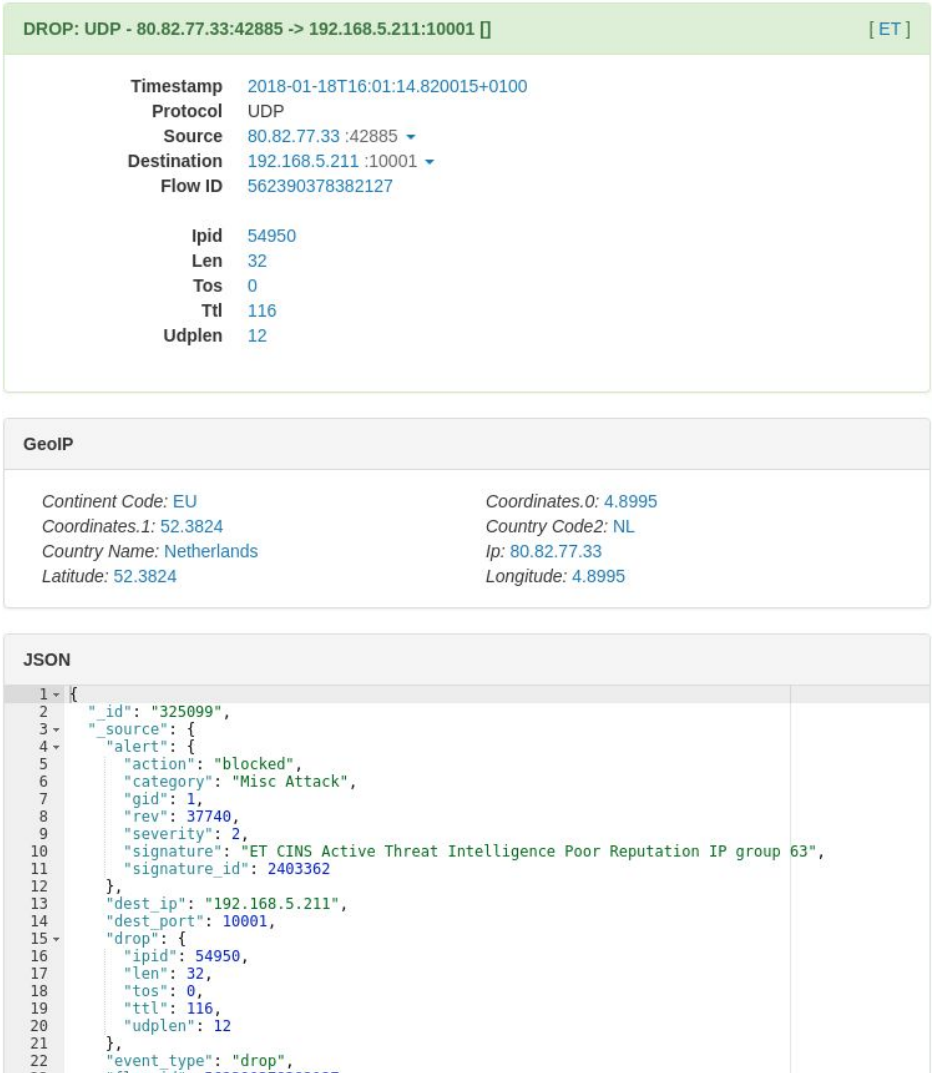
signature_id

gid

Signature: ET XXXX

xff

Se HTTP e proxy -> squid/access.log



DROP: UDP - 80.82.77.33:42885 -> 192.168.5.211:10001 [] [ET]

Timestamp	2018-01-18T16:01:14.820015+0100
Protocol	UDP
Source	80.82.77.33 :42885
Destination	192.168.5.211 :10001
Flow ID	562390378382127
Ipid	54950
Len	32
Tos	0
Ttl	116
Udplen	12

GeoIP

Continent Code: EU
Coordinates.1: 52.3824
Country Name: Netherlands
Latitude: 52.3824
Coordinates.0: 4.8995
Country Code2: NL
Ip: 80.82.77.33
Longitude: 4.8995

JSON


```
{
  "_id": "325099",
  "_source": {
    "alert": {
      "action": "blocked",
      "category": "Misc Attack",
      "gid": 1,
      "rev": 37740,
      "severity": 2,
      "signature": "ET CINS Active Threat Intelligence Poor Reputation IP group 63",
      "signature_id": 2403362
    },
    "dest_ip": "192.168.5.211",
    "dest_port": 10001,
    "drop": {
      "ipid": 54950,
      "len": 32,
      "tos": 0,
      "ttl": 116,
      "udplen": 12
    },
    "event_type": "drop",
```

Firme /2

3 opzioni per ogni categoria: Disabilita / Allarme / Blocca

Gestione singole regole nelle categorie -> pulledpork

Disabilitazione regole per determinati IP -> suricata

/etc/pulledpork/disablesid.conf

```
# FP - ET TROJAN Win32\/Ropest.H CnC - INBOUND set
1:2025068
# FP - ET MALWARE Executable purporting to be .txt file with no Referer - Likely Malware on
fedoraproject.org/static/hotspot.txt
1:2010500
```

Anatomia di una regola

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET INFO Session Traversal Utilities for NAT (STUN Binding Response)"; content:"|01 01 00 44|"; depth:4; content:"|00 01 00 08|"; distance:16; within:4; threshold:type limit, track by_src, count 1, seconds 60; reference:url,tools.ietf.org/html/rfc5389; classtype:protocol-command-decode; sid:2018908; rev:2; metadata:created_at 2014_08_07, updated_at 2014_08_07;)

https://github.com/OISF/suricata/blob/master/classification.config

/etc/e-smith/templates-custom/etc/suricata/threshold.config/90stun

```
# ET INFO Session Traversal Utilities for NAT (STUN Binding Response) gigaset a510 ip
suppress gen_id 1, sig_id 2018908, track by_src, ip 192.168.5.87
suppress gen_id 1, sig_id 2018908, track by_dst, ip 192.168.5.87
```

Conclusioni

Ciclo continuo Allarme - Verifica FP - Disabilitazione/soppressione

Idealmente 0 Allarmi (vedere report settimanale)

Conteggio bloccaggi per verifica efficacia

Forum per condividere esperienze e case study

Live (IMAPS, CVE-2016-2211, Masscan d-link, JAR size)

Domande