Corso di Sicurezza delle Reti e dei Sistemi Software *aa 2015/16*

Universita' degli Studi del Sannio

Ing. Antonio Pirozzi

Projectwork

Si realizzi un tool in python, che prenda in INPUT le Snort Rules e le traduca in Rules iptables.
Il tool dovra' avere I seguenti requirements:

Supported options: [--log] [--drop| --reject]
Acting as a system daemon...
Print the results of translation as fwsnort do
…..

Some bg

IPS≠ firewall

Some Issues:
- Snort DCE/RPC Preprocessor vulnerability
- Host fragment reassembly
- Stick/Snot DoS

Similar tools:
- fwsnort
- http://www.stearns.org/snort2iptables/

Snort is a free and opensource network intrusion prevention system (NIPS) and network intrusion detection system (NIDS)

- analyzes the packets passing over the network,
- comparing them with a database of attack signatures;
- earns to recognize new attacks, by introducing new signatures recognized as attacks;
- verify the protocols used by the packets, so as to recognize any anomalies in the traffic;
- detects the activity of the port scan, "exploration", which generally precedes an attack

The general form of a Snort rule :

action proto src_ip src_port direction dst_ip dst_port (options)

Iptables: application layer data

Matching Printable DATA :

1

```
iptables -I INPUT 1 -p tcp --dport 5001 -m string --string "tester"
--algo bm -m state --state ESTABLISHED -j LOG --log-prefix "tester"
```

Matching NON Printable (bytes) DATA :

2

```
iptables -I INPUT 1 -p udp --dport 5002 -m string --hex-string
"|a7a7a7a7a7a7a7a7a7a7|" --algo bm -j LOG --log-prefix "YEN "
```

From Linux Firewalls By Michael Rash
Publisher : No Starch Press

Iptables: application layer data

Matching BoF Attack :

```
iptables -I FORWARD 1 -p tcp --dport 443 --algo bm -m state
-m state --state
ESTABLISHED -m string --string "AAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" -j LOG
--log-prefix "SSL BoF detected "
```

From Linux Firewalls By Michael Rash
Publisher : No Starch Press

Some examples..

From SNORT rules to iptables :

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg: "BLEEDING-EDGE EXPLOIT MS-SQL SQL Injection closing string plus line comment"; flow: to_server,established; content:"'|00|"; content:"-|00|-|00|"; reference:url,www.nextgenss.com/papers/more_advanced_sql_injection.pdf; reference:url,www.securitymap.net/sdm/docs/windows/mssql-checklist.html; classtype: attempted-user; sid: 2000488; rev:5;)

---

iptables -I FORWARD 1 -p tcp --dport 1433 -m state --state ESTABLISHED -m string --hex-string "'|00|" --algo bm -m string --hex-string "-|00|-|00|" --algo bm -j LOG --log-prefix "SQL INJECTION COMMENT "

From Linux Firewalls By Michael Rash
Publisher : No Starch Press

Limits

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHOWN overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"CHOWN"; distance:0; nocase; isdataat:100,relative; pcre:"/^SITE\s+CHOWN\s[^\n]{100}/smi"; reference:bugtraq,2120; reference:cve,2001-0065; classtype:attempted-admin; sid:1562; rev:11;)

20 bytes for the IP header
and 20 bytes for the TCP header

[iptablesfw]# iptables -I FORWARD 1 -p tcp --dport 21 -m state --state ESTABLISHED -m string --string "site" --algo bm -m string --string "chown" --algo bm -m length --length 140 -j LOG --log-prefix "CHOWN OVERFLOW "

From Linux Firewalls By Michael Rash
Publisher : No Starch Press

References/resources:

1 Advanced Linux Firewalls
Michael Rash
Security Architect
Enterasys Networks, Inc.

2 https://cipherdyne.org/talks/**Advanced_Linux_Firewalls.pdf**