Ασφάλεια Συστημάτων και Υπηρεσιών - ΗΡΥ 413

Αστερινός Καράλης – Ζωγραφούλα Ιωάννα Νεαμονιτάκη

Part 3

Παρακάτω φαίνονται οι κανόνες που γράφτηκαν στο part 3:

1.

**alert tcp any any -> 192.168.1.1 54321 (content:"Faye-0088"; msg:"Student Packet Detected"; sid:1000001; rev:1;)**

Ο παραπάνω κανόνας είναι για την πραγματοποίηση ενός alert όταν εντοπίζεται το student packet, δηλαδή ένα πακέτο που στέλνεται με TCP πρωτόκολλο από οποιαδήποτε τυχαία IP και τυχαίο port (any any) προς την IP **192.168.1.1** και στο port **54321** με περιεχόμενα “**Faye-0088**”.

2.

**alert tcp any any -> 192.168.1.2 80 (msg:"Port Scan Packet Detected - HTTP"; sid:1000002; rev:1;)**

**alert tcp any any -> 192.168.1.2 443 (msg:"Port Scan Packet Detected - HTTPS"; sid:1000003; rev:1;)**

**alert tcp any any -> 192.168.1.2 22 (msg:"Port Scan Packet Detected - SSH"; sid:1000004; rev:1;)**

**alert tcp any any -> 192.168.1.2 23 (msg:"Port Scan Packet Detected - TELNET"; sid:1000005; rev:1;)**

**alert tcp any any -> 192.168.1.2 21 (msg:"Port Scan Packet Detected - FTP"; sid:1000006; rev:1;)**

**alert tcp any any -> 192.168.1.2 53 (msg:"Port Scan Packet Detected - DNS"; sid:1000007; rev:1;)**

**alert tcp any any -> 192.168.1.2 554 (msg:"Port Scan Packet Detected - RTSP"; sid:1000008; rev:1;)**

**alert tcp any any -> 192.168.1.2 1433 (msg:"Port Scan Packet Detected - SQL"; sid:1000009; rev:1;)**

**alert tcp any any -> 192.168.1.2 3389 (msg:"Port Scan Packet Detected - RDP"; sid:1000010; rev:1;)**

**alert tcp any any -> 192.168.1.2 1883 (msg:"Port Scan Packet Detected - MQTT"; sid:1000011; rev:1;)**

Τα παραπάνω alerts είναι για το port scan packet. Βρέθηκαν ποια ports χρησιμοποιούνται για κάθε πρωτόκολλο και παρατίθενται παρακάτω:

* **HTTP -> 80**
* **HTTPS -> 433**
* **SSH -> 22**
* **TELNET -> 23**
* **FTP -> 21**
* **DNS -> 53**
* **RTSP -> 554**
* **SQL -> 1433** (όταν στέλνεται μέσω TCP)
* **RDP -> 3389**
* **MQTT -> 1883**

Οπότε ο παραλήπτης του πακέτου έχει IP **192.168.1.2** και ότι port έχει το πρωτόκολλο.

3.

**alert tcp any any -> 192.168.1.3 8080 (content:"MTIzNDU2Nzg5MA=="; msg:"Base64 Malicious Packet Detected"; sid:1000012; rev:1;)**

Αυτός ο κανόνας είναι για να εντοπίσει μόνο 1 από τα 5 πακέτα που στάλθηκαν με encoding Base64. Αν θέλαμε να βγάλει alert και για τα άλλα 4 πακέτα θα έπρεπε να βγάλουμε το πεδίο **content** και θα εντοπίζαμε όλα τα πακέτα που είχαν παραλήπτη μεIP **192.168.1.3** και port **8080.**4.

**alert udp any any -> 127.0.0.53 53 (msg:"DNS Suspicious Domain Packet Detected"; sid:1000013; rev:1;)**

Η διαφορά από τους προηγούμενους κανόνες είναι πως εδώ ο κανόνας εντοπίζει UDP πρωτόκολλο αντί για TCP. Κάνει trigger το alert όταν δει πακέτο προς παραλήπτη με IP **127.0.0.53** και port 53. Ο αποστολέας μπορεί να έχει οποιαδήποτε IP και οποιοδήποτε port.

5.

**alert icmp any any -> any any (content:"PingTest-2024"; msg:"ICMP Ping Packet Detected"; sid:1000014; rev:1;)**

Τέλος ο κανόνας εντοπίζει ICMP πρωτόκολλο από οποιαδήποτε IP και port ως αποστολέα αλλά και οποιαδήποτε IP και port ως παραλήπτη με περιεχόμενο πακέτου PingTest-2024.

Παρακάτω φαίνονται όλα τα alerts που δημιουργούνται τρέχοντας την εντολή:

**snort -q –-talos -r custom\_packet.pcap**

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα