Snort Rules for Assignment 7

1. alert tcp any any -> 192.168.1.1 54321 (msg:"Student Packet Detected"; content:"Michail\_Kratimenos-2018030104"; sid:1000001; rev:1;)

Αυτός ο κανόνας εντοπίζει ένα πακέτο TCP που έχει σταλεί στη διεύθυνση IP: 192.168.1.1 και στο port: 54321, όπως και ζητήθηκε. Ο κανόνας ψάχνει το συνδυασμό του ονοματεπωνύμου μου και του ΑΜ μου και επαληθεύει τη σωστή δημιουργία του προσαρμοσμένου πακέτου όπως καθορίζεται στην ανάθεση.

2\_1. alert tcp any any -> 192.168.1.2 80 (msg:"HTTP Port Scan Detected"; sid:1000002; rev:1;)

2\_2. alert tcp any any -> 192.168.1.2 443 (msg:"HTTPS Port Scan Detected"; sid:1000003; rev:1;)

2\_3. alert tcp any any -> 192.168.1.2 22 (msg:"SSH Port Scan Detected"; sid:1000004; rev:1;)

2\_4. alert tcp any any -> 192.168.1.2 23 (msg:"TELNET Port Scan Detected"; sid:1000005; rev:1;)

2\_5. alert tcp any any -> 192.168.1.2 21 (msg:"FTP Port Scan Detected"; sid:1000006; rev:1;)

2\_6. alert tcp any any -> 192.168.1.2 53 (msg:"DNS Port Scan Detected"; sid:1000007; rev:1;)

2\_7. alert tcp any any -> 192.168.1.2 554 (msg:"RTSP Port Scan Detected"; sid:1000008; rev:1;)

2\_8. alert tcp any any -> 192.168.1.2 3306 (msg:"SQL Port Scan Detected"; sid:1000009; rev:1;)

2\_9. alert tcp any any -> 192.168.1.2 3389 (msg:"RDP Port Scan Detected"; sid:1000010; rev:1;)

2\_10. alert tcp any any -> 192.168.1.2 1883 (msg:"MQTT Port Scan Detected"; sid:1000011; rev:1;)

Αυτοί οι κανόνες εντοπίζουν πακέτα TCP που έχουν σταλεί στη διεύθυνση IP: 192.168.1.2 και στα ports: 80, 443, 22, 23, 21, 53, 554, 3306, 3389, 1883, για τις υπηρεσίες: HTTP, HTTPS, SSH, TELNET, FTP, DNS, RTSP, SQL, RDP, MQTT αντίστοιχα. Τα ports αυτά επιλέχθηκαν καταλλήλως από την εξής πηγή: <https://sumofbytes.com/blog/cheatsheet-default-ports-of-popular-databases-and-network-internet-protocols>. Αυτοί οι κανόνες βοηθούν στην παρακολούθηση αναγνωριστικών δραστηριοτήτων μέσα σε ένα δίκτυο. Στο screenshot φαίνεται ότι έχει προκληθεί ένα alert για κάθε υπηρεσία.

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

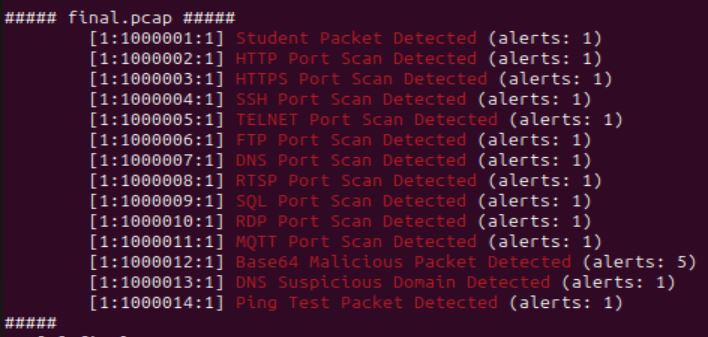
Αυτός ο κανόνας αναγνωρίζει ένα TCP πακέτο με διεύθυνση IP παραλήπτη: 192.168.1.3 και port: 8080. Το base64-κωδικοποιημένο ονοματεπώνυμο και ΑΜ μου ελέγχεται ότι είναι σωστό. Έτσι, ανιχνεύονται πιθανά κακόβουλα περιεχόμενα στην κίνηση του δικτύου. Τέλος, στο screenshot φαίνονται 5 ειδοποιήσεις, καθώς από τον κώδικα 5 πακέτα στάλθηκαν, όπου τα 4 από αυτά ήταν retransmissions του πρώτου.

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

Αυτός ο κανόνας αντιστοιχεί σε ένα ερώτημα DNS για το malicious.example.com στο port 53. Η διεύθυνση IP του VM βρήκαμε ότι είναι η 127.0.0.53 με τη χρήση της εντολής: cat /etc/resolv.conf. Δείχνει τη δυνατότητα αναγνώρισης αιτημάτων DNS για δυνητικά επιβλαβείς τομείς, κάτι που αποτελεί κοινή ένδειξη κακόβουλου λογισμικού ή διείσδυσης. Στη δική μας περίπτωση ωστόσο αν βάζαμε σαν όρισμα το content = malicious.example.com δεν προκαλούνταν κάποια ειδοποίηση στην οθόνη, οπότε το βγάλαμε και λειτούργησε, αν και μάλλον δεν είναι σωστός κανόνας και πιθανότατα ανιχνεύει και άλλες περιπτώσεις που δε θα έπρεπε.

5. alert icmp any any -> 192.168.1.4 any (msg:"Ping Test Packet Detected"; content:"PingTest-2024"; sid:1000014; rev:1;)

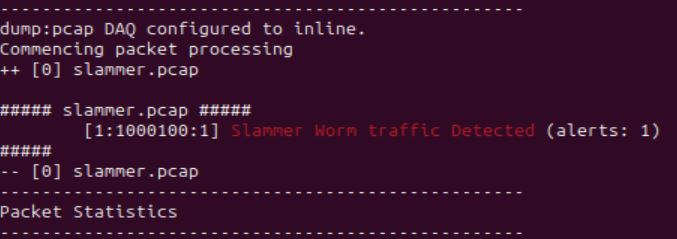
Αυτός ο κανόνας εντοπίζει πακέτα ICMP (ping) που αποστέλλονται στη διεύθυνση IP: 192.168.1.4 με το κείμενο: "PingTest-2024". Μέσω αυτού, φαίνεται η δυνατότητα παρακολούθησης της κυκλοφορίας ICMP, η οποία μπορεί να χρησιμοποιηθεί για διάγνωση ή αναγνώριση.



Slammer Worm:

alert udp any any -> 65.165.167.86 1434 (msg:"Slammer Worm traffic Detected"; content:"\x01" sid:1000100; rev:1;)

Αυτός ο κανόνας είναι ειδικά σχεδιασμένος για το Slammer Worm. Ψάχνει πακέτα UDP που έχουν ως προορισμό τη διεύθυνση IP: 65.165.167.86 και το port: 1434, τα οποία τα βρήκαμε από το pcap αρχείο slammer. Το port 1434 είναι σημαντικό, καθώς το Slammer Worm εμφανίζει μια buffer overflow αδυναμία στον Microsoft SQL Server, η οποία ακούει σε αυτό το port. Ο κανόνας ελέγχει για το byte \x01, το οποίο είναι χαρακτηριστικό των πακέτων Slammer Worm.

Στο παρακάτω screenshot επιβεβαιώνεται ότι ο κανόνας βρήκε ένα Slammer Worm πακέτο στο slammer.pcap αρχείο

Η ανίχνευση αυτή διασφαλίζει ότι οποιαδήποτε παρόμοια κακόβουλη δραστηριότητα μπορεί να εντοπιστεί και να επισημανθεί σε πραγματικό χρόνο ή κατά τη διάρκεια της ανάλυσης.