Ασφάλεια στο Υπολογιστικό Νέφος

- Εισβολή Ασφάλειας (*Security Intrusion*): Ένα συμβάν ασφαλείας ή συνδυασμός πολλαπλών συμβάντων ασφάλειας, όπου ο εισβολέας αποκτά ή επιχειρεί να αποκτήσει πρόσβαση σε ένα σύστημα (ή σε πόρους του συστήματος) χωρίς να έχει άδεια για να το κάνει.

- Ανίχνευση Εισβολής (*Intrusion Detection*): Η υπηρεσία ασφαλείας που παρακολουθεί και αναλύει γεγονότα του συστήματος με σκοπό την ανίχνευση/διαπίστωση και την παροχή προειδοποίησης σε(σχεδόν) πραγματικό χρόνο, τυχόν προσπαθειών χρηστών να αποκτήσουν πρόσβαση σε πόρους του συστήματος με μη εξουσιοδοτημένο τρόπο.

- Έκθεση Υπηρεσίας(*Compromised Service)*: Η υπηρεσία η οποία λειτουργεί σε ένα υπολογογιστικό σύστημα έχει εκτεθεί λόγω επιτυχημένης επίθεσης και τον έλεγχο της, τον κατέχει ο εισβολέας.

Κατηγορίες εισβολέων

Μια από τις πιο ευρέως δημοσιοποιημένες απειλές της ασφάλειας ενός συστήματος είναι οι εισβολείς, οι οποίοι συχνά αναφέρονται ως hacker ή cracker. Παρακάτω ακολουθεί η πρώτη κατάταξη εισβολέων.

- **Μεταμφιεσμένος** (*Masquerader*): Άτομο που δεν είναι εξουσιοδοτημένο να χρησιμοποιήσει τον υπολογιστή και διαπερνά τον έλεγχο πρόσβασης του συστήματος για να εκμεταλλευτεί το λογαριασμό ενός νομίμου χρήστη. Είναι συνήθως outsider.
- **Παράνομος** (*Misfeasor*): Νόμιμος χρήστης που προσπελαύνει δεδομένα, προγράμματα ή πόρους που δεν είναι εξουσιοδοτημένος να προσπελάσει ή δεν ειναι εξουσιοδοτημένος για αυτήν την πρόσβαση, αλλά καταχράται τα προνόμιά του. Είναι συνήθως insider.
- **Λαθραίος Χρήστης** (*Clandestine user*): Άτομο που παίρνει έλεγχο του συστήματος και τον χρησιμοποιεί για να αποφύγει ή να καταστείλει τον έλεγχο πρόσβασης. Μπορεί να είναι είτε insider, είτε outsider.

Κατηγορίες εισβολέων (συν.)

Το είδος των εισβολέων καθορίζει το επίπεδο βλάβης το οποίο μπορεί να επιτευχθεί σε μια επίθεση.

Σύγχρονη κατηγοριοποίηση των εισβολέων

- Χάκερ με ελάχιστες τεχνικές δεξιότητες(script kiddies)
- Χάκερ με επαρκείς τεχνικές γνώσεις
- Χακτιβιστές (hactivists)
- Συντονισμένες ομάδες χάκερ
- Κυβερνητικές υπηρεσίες πληροφοριών

Οι δραστηριότητες των εισβολέων περιλαμβάνουν:

- Κλοπή προσωπικών δεδομένων
- Εταιρική κατασκοπεία
- Κλοπή διαπιστευτηρίων
- Κλοπή ταυτοτήτων
- Κλοπή κρατικών πληροφοριών υπηρεσιών

Ανίχνευση εισβολών

- Αν ανιχνευτεί μια αρκετά γρήγορα, μπορεί να προσδιοριστεί η ταυτότητα του εισβολέα και να απομακρυνθεί από το σύστημα πριν γίνει ζημιά ή αποκαλυφθούν δεδομένα που διαχειρίζονται.

- Ένα αποτελεσματικό σύστημα ανίχνευσης εισβολών μπορεί να παίξει επίσης το ρόλο εμποδίου, λειτουργώντας έτσι ώστε να αποτρέπει εισβολές. (IPS)

- Η ανίχνευση εισβολών επιτρέπει τη συλλογή πληροφοριών σχετικά με τις τεχνικές εισβολής, οι οποίες μπορούν να χρησιμοποιηθούν για αν ισχυροποιήσουν τις μεθόδους παρεμπόδισης εισβολών.

Συστήματα Ανίχνευσης Εισβολών

- Host-based IDS: Παρακολουθεί τα χαρακτηριστικά ενός συγκεκριμένου μηχανήματος(host) για ύποπτη δραστηριότητα.

- Network-based IDS: Παρακολουθεί την κίνηση του δικτύου και αναλύει πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογής για τον εντοπισμό ύποπτης δραστηριότητας.

- Κατανεμημένο(distributed) ή υβριδικό IDS: Συνδυάζει πληροφορίες από μια σειρά αισθητήρων, σε έναν κεντρικό αναλυτή που είναι σε θέση να εντοπίσει καλύτερα και να απαντήσει σε δραστηριότητα εισβολής.

Δολώματα (honeypots)

- Συστήματα παραπλάνησης που εφαρμόζονται σε μεμονωμένα ή κατανεμημένα συστήματα και είναι σχεδιασμένα για να παρασύρουν εισβολείς.
- Εκθέτουν κατασκευασμένες πληροφορίες οι οποίες είναι φτιαγμένες να μοιάζουν πολύτιμες και τις οποίες οι νόμιμοι χρήστες μιας υποδομής δεν θα τις χρησιμοποιούσαν.
- Όταν οι χάκερ είναι εντός του δικτύου, οι διαχειριστές έχουν την δυνατότητα παρατήρησης της συμπεριφοράς τους και απομόνωσής τους.

Επιθέσεις

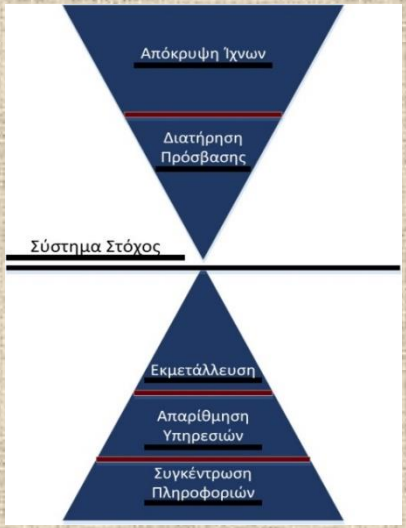
Είδη επιθέσεων

- Άρνηση παροχής υπηρεσιών (DDoS)
- Μηδενικής ημέρας (0-day)
- Επίμονες επιθέσεις (APT)
- Αναχαίτηση διαδικτυακού παρόχου
- Κοινωνική μηχανική (social engineering)
- Διαφυγή συστήματος εικονικοποίησης(VM breakout) και
- Αυτοματοποιημένα εργαλεία εκμετάλλευσης.

Φάσεις Επίθεσης

Η διεξαγωγή μιας επίθεσης ανεξάρτητα από το είδος στο οποίο ανήκει αποτελείται από πέντε φάσεις:

- Συγκέντρωση πληροφοριών
- Απαρίθμηση υπηρεσιών
- Εκμετάλλευση
- Διατήρηση πρόσβασης
- Απόκρυψη ίχνων.



Μεθοδολογία Διείσδυσης

Δριμύτητα τρωτών σημείων

Σύμφωνα με το NVD , το οποίο αποτελεί το εθνικό αποθετήριο προτύπων διαχείρισης τρωτών σημείω
ν των Ηνωμένων Πολιτειών της Αμερικής, ο βαθμός επικινδυνότητας των τρωτών σημείων υπολογίζετ
αι μέσω ενός συστήματος βαθμονόμησης τρωτών σημείων, το CVSS.

Δριμύτητα	**CVSS score**
Περιορισμένη-Συγκέντρωση Πληροφοριών μόνο	0
Χαμηλή	1.0-3.9
Μέτρια	4.0-6.9
Υψηλή	7.0-10.0

Τρωτά σημεία και έκθεση (CVE)

Τα κενά και τα λάθη του λογισμικού τα οποία επιτρέπουν την εκμετάλλευση και κατ'επέκταση την παραβίαση μιας πολιτικής ασφάλειας χαρακτηρίζονται ως CVEs. Ενα σύστημα ή μια υποδομή λόγω των CVEs, μπορεί να βρεθεί σε κατάσταση έκθεσης. Σε αυτήν την κατάσταση πλέον ο εισβολέας έχει καταλάβει ύπο τον έλεγχό του το τμήμα της υποδομής ή του συστήματος το οποίο έχει προσβληθεί από την επίθεση του και οι δυνατότητες αυτού επιβοηθούν τον εισβολέα στην περαιτέρω εκμετάλλευση. Μερικές επίμονες επιθέσεις και τα CVEs τους είναι τα ακόλουθα:

- cve-2010-2772 **stuxnet**
- cve-2012-1889 **flame**
- cve-2011-3402 **duqu**

Κακόβουλο Λογισμικό

- **Ιός**: Προσαρτά τον εαυτό του σε ένα πρόγραμμα και μεταδίδει αντίγραφα του εαυτού του σε άλ λα προγράμματα.
- **Μακροιός**: Τύπος ιού που χρησιμοποιεί κώδικα γραμμένο με μακροεντολές και αποτελεί μέρος ενός εγγράφου.
- **Σκουλήκι**: Πρόγραμμα που μεταδίδει αντίγραφα του εαυτού του σε άλλους υπολογιστές.
- **Λογική Βόμβα**: Εκκινεί κάποια ενέργεια όταν ικανοποιηθεί μια συνθήκη η οποία ορίζεται από τ ον εισβολέα.
- **Κερκόπορτα**: Τροποποίηση προγράμματος έτσι ώστε να επιτρέπεται μη εξουσιοδοτημένη πρόσ βαση και εκτέλεση λειτουργιών.

Κακόβουλο Λογισμικό (συν.)

- **Δούρειος Ίππος**: Πρόγραμμα που εκτελεί κάποια επιπλέον λειτουργία, μη αναμενόμενη και βλα πτική για το σύστημα που εκτελείται.
- **Flooder**: Χρησιμοποιείται για επίθεση σε δικτυωμένα υπολογιστικά συστήματα που διακινούν μ εγάλο όγκο πληροφορίας, προκειμένου να εκτελεέσουν DDoS επίθεση.
- **Rootkit**: Σύνολο εργαλείων των χάκερ που χρησιμοποιείται εφόσον ο εχθρός έχει διεισδύσει σε ένα υπολογιστικό σύστημα και έχει αποκτήσει πρόσβαση ως διαχειριστής (root).
- **Zombie**: Πρόγραμμα που ενεργοποιείται σε ένα ήδη μολυσμένο μηχάνημα ώστε να εξαπολύσει επιθέσεις σε άλλα μηχανήματα.
- **Exploit**: Κώδικας που προσπαθεί να εκμεταλλευτεί ένα ή περισσότερα τρωτά σημεία.

Δομή ιού

- Ο ιός προσαρτάται μέσα σε ένα εκτελέσιμο πρόγραμμα στην αρχή του ώστε να εκτελεστεί πρώτ ος και στην συνέχεια ο κώδικας του προγράμματος.
- Η πρώτη γραμμή του κώδικα παρέχει έναν δείκτη που χρησιμεύει στον να προσδιορίσει ο ιός αν το πρόγραμμα είναι ήδη μολυσμένο ή όχι.
- Στην συνέχεια με την εκτέλεση του προγράμματος εκτελείται και ο ιός ή θα μπορούσε να συνδυ αστεί με μια λογική βόμβα και να εκτελείται μόνο σε περίπτωση που συγκεκριμένες συνθήκες τ ου περιβάλλοντος εκτέλεσης ικανοποιούνται.
- Είναι σχεδόν αδύνατη η ανίχνευσή τους από τους χρήστες και η ανίχνευσή τους βασίζεται στον έλεγχο του μήκους ενός προγράμματος.

Φάσεις ζωής ιού

Κατά την διάρκεια ζωής του, ένας ιός διανύει τις ακόλουθες τέσσερις φάσεις:

- **Λανθάνουσα Φάση**: Ο ιός είναι ανενεργός. Θα ενεργοποιηθεί από κάποιο γεγονός, όπως ημερ ομηνία ή υπέρβαση της χωρητικότητας του δίσκου.
- **Φάση Διάδοσης**: Ο ιός τοποθετεί ένα ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε ορισμένες περιοχές του συστήματος.
- **Φάση Πυροδότησης**: Ο ιός ενεργοποιείται για να υλοποιήσει τη λειτουργία για την οποία κατασ κευάστηκε.
- **Φάση Εκτέλεσης**: Πραγματοποιείται η λειτουργία η οποία φαινομενικά μπορεί να είναι αβλαβή ς αλλά να πραγματοποιεί επιβλαβής ενέργειες όπως καταστροφή αρχείων.

Τύποι Ιών

- **Παρασιτικός ιός**: Προσαρτά τον εαυτό του σε εκτελέσιμα αρχεία και δημιουργεί αντίγραφα του.
- **Ιός έμφυτος στην κύρια μνήμη**: Διατηρείται στην κύρια μνήμη και μολύνει τα προγράμματα πο υ εκτελούνται.
- **Αόρατος ιός**: Μορφή σχεδιασμένη κατάλληλα ώστε να προστατεύει τον εαυτ΄’ο του από αντιβιο τικά και προγράμματα ανίχνευσης.
- **Πολυμορφικός ιός**: Ιός που μεταλλάσεται με κάθε μόλυνση, κάνοντας αδύνατη την ανίχνευσή τ ου μέσω της υπογραφής του.

Δικτυακά Σκουλήκια

Τα δικτυακά σκολήκια εμφανίζουν τα ίδια χαρακτηριστικά και φάσεις με τους ιούς υπολογιστών.

Γνωστά δικτυακά σκουλήκια:

- **Σκουλήκι του Morris**: εξαπλωνόταν σε συστήματα UNIX και η ανίχνευση στόχων γινόταν από τους πίνακες δρομολόγησης των ήδη προσβεβλημένων συστημάτων.
- **Code Red 2**: έχει σαν στόχο τους διακομιστές IIS της Microsoft και εγκαθιστά μια κερκόπορτα επιτρέποντας στους χάκερ να καταγράψουν τις δραστηριότητες των χρηστών υπολογιστών-θυμάτων.
- **Nimba**: τροποποιεί έγγραφα του Ιστού και ορισμένα εκτελέσιμα αρχεία που βρίσκει στα συστήματα που μολύνει.
- **SQL Slammer**: εκμεταλλεύεται ένα τρωτό σημείο υπερχείλισης της προσωρινής μνήμης (buffer overflow) στους διακομιστές SQL της Microsoft.

Δούρειος Ίππος

Ο δούρειος ίππος είναι ένα φαινομενικά χρήσιμο πρόγραμμα το οποίο διαθέτει επιβλαβή κώδικα ο οπ οίος δημιουργεί ξημιά στο υπολογιστικό σύστημα που εκτελείται.

Ενέργειες δούρειου ίππου:

- Εκτελεί την λειτουργία του προγράμματος στο οποίο είναι προσκολλημένος και στην συνέχεια δι ενεργεί επιπρόσθετες επιβλαβείς εργασίες.
- Εκτελεί το πρόγραμμα με τροποποιήσεις.
- Εκτελεί διαφορετική λειτουργία από αυτήν που υποτίθεται πως θα έπρεπε να εκτελεί.

Παράδειγμα δούρειου ίππου είναι ο GPCode ο οποίος κρυπτογραφεί επιλεγμένα αρχεία και ο εισβολέ ας στη συνέχεια απαιτεί χρηματική αμοιβή πρός την αποκρυπτογράφησή τους.

Μέτρα Αντιμετώπισης

- **Ανίχνευση**: Μόλις ένα μηχάνημα μολυνθεί, πρέπει να γίνει αντιληπτό και να υπάρξει εντοπισμός του κακόβουλου λογισμικού.
- **Προσδιορισμός ταυτότητας**: Μόλις επιτευχθεί η ανίχνευση, πρέπει να ταυτοποιηθεί το λογισμικ ό που προκάλεσε την μόλυνση.
- **Απομάκρυνση**: Μόλις αναγνωριστεί το συγκεκριμένο κακόβουλο λογισμικό, πρέπει να απομακρ υνθεί προκειμένου να επανέλθει το σύστημα.

Σε περίπτωση που ανιχνευτεί το κακόβουλο λογισμικό αλλά δεν επιτευχθεί αναγνώριση και απομάκρυ νση του τότε το προγραμμα ή το σύστημα που έχει προσβληθεί πρέπει να αντικατασταθεί από εφεδρι κή έκδοση.

Τείχη Προστασίας

Το τείχος προστασίας παρεμβάλλεται μεταξύ του εσωτερικού δικτύου μια υποδομής και του διαδικτύου, εγκαθιδρύωντας μια ελεγχόμενη ζεύξη στην οποία μπορούν να εφαρμοστούν πολιτικές ασφάλειας.

- Όλη η δικτυακή κίνηση ανεξάρτητα από την κατεύθυνση της περνά μέσα από το τείχος προστασίας.
- Μόνο εξουσιοδοτημένη κίνηση επιτρέπετε αλλιώς μπλοκάρεται από τις πολιτικές ασφάλειας.
- Αποτελεί μοναδικό σημείο ελέγχου κατεύθυνσης κίνησης, χρηστών και συμπεριφοράς των χρηστών.
- Δεν μπορεί να προστατεύσει από επιθέσεις που το παρακάμπτουν.
- Δεν προστατεύει από εσωτερικές απειλές.

Φιλτράρισμα πακέτων στα τείχη προστασίας

Οι τύποι τειχών προστασίας ορίζονται από το σύνολο κανόνων που εφαρμοζουν στα εισερχόμενα και εξερχόμενα πακέτα. Τα εξεταζόμενα πεδία στα οποία εφαρμοζονται οι κανόνες είναι:

- IP Διεύθυνση Πηγής
- IP Διεύθυνση Προορισμού
- Διεύθυνση Πηγής και Προορισμού επιπέδου μεταφοράς: η θύρα του επιπέδου μεταφοράς προσ διορίζει εφαρμοφές τύπου SNMP και telnet.
- Πεδίο πρωτοκόλλου: Ορίζει το πρωτόκολλο μεταφοράς.
- Διασύνδεση: Προσδιορίζεται από ποια διασύνδεση ή διεπαφή του τείχους προστασίας προήλθε ή μέσω ποιας θα αποσταλεί ένα πακέτο.

Εργαλεία συγκέντρωσης πληροφοριών(Φάση 1)

- **Nessus**

  Το nessus είναι εργαλείο αξιολόγησης και ανίχνευσης τρωτών σημείων, όπως επίσης και διαχείρισης των απειλών. Το nessus έχει την δυνατότητα σάρωσης θυρών, λειτουργικών συστημάτων, συστημάτων εικονικοποίησης, κακόβουλου λογισμικού και συλλογής ευαίσθητων πληροφοριών.

- **OpenVAS**

  Το OpenVAS είναι ένα σύμπλεγμα εργαλείων και υπηρεσιών σάρωσης τρωτών σημείων και διαχείρισης αυτών. Το OpenVAS διατηρεί ένα δημόσιο αποθετήριο προτάσεων και δοκιμών για τον έλεγχο τρωτών σημείων και μέσω αυτών πραγματοποιούνται οι σαρώσεις.

- **Metasploit**

  Το Metasploit είναι μια πλατφόρμα ελέγχου διείσδυσης βασισμένη στη γλώσσα προγραμματισμού Ruby, η οποία επιτρέπει τη συγγραφή και την δημιουργία κώδικα εκμετάλλευσης όπως επίσης και σάρωσης τρωτών σημείων ενός υπολογιστικού συστήματος. Η πλατφόρμα είναι συνδεδεμένη με βάση δεδομένων για την ανεύρεση κώδικα εκμετάλλευσης, ανίχνευσης, αποφυγής ανίχνευσης, αύξησης προνομίων και σάρωσης.

Εργαλεία συγκέντρωσης πληροφοριών(Φάση 1) (συν.)

- **Nmap**

  Το nmap είναι εργαλείο σάρωσης δικτύων για την ανεύρεση πληροφοριών σχετικά με τα υπολογιστικά συστήματα είναι συνδεδεμένα σε αυτά. Μέσω της δυνατότητας nmap scripting engine είναι εφικτή η αυτοματοποίηση έλεγχων και σαρώσεων με την συγγραφή scripts όπως επίσης είναι δυνατή η ανεύρεση γνωστών τρωτών σημείων μέσω των nse scripts του εργαλείου.

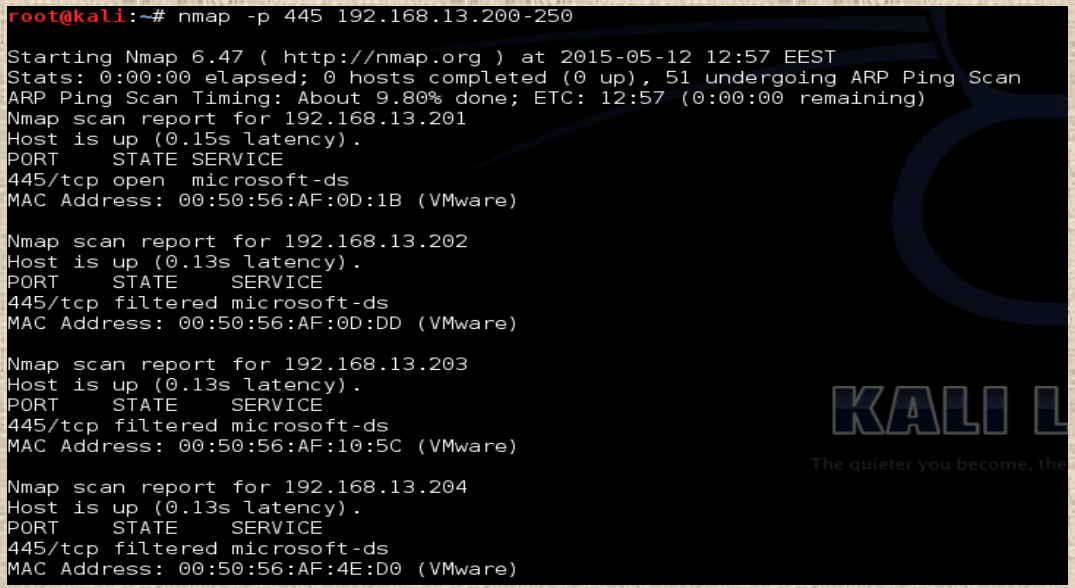
- **SpiderFoot**

  Το SpiderFoot αποτελεί εργαλείο ελεύθερου λογισμικού αυτοματοποιημένης συγκέντρωσης πληροφοριών. Μέσω προκαθορισμένων ελέγχων και σαρώσεων συγκεντρώνονται πληροφορίες και πραγματοποιείται σάρωση των θυρών όπως επίσης και αξιολόγηση τρωτών σημείων.

- **Tcpdump, Wireshark**

  Το εργαλεία tcpdump και wireshark είναι αναλυτές πακέτων και δικτυακής κίνησης. Τα συγκεκριμένα εργαλεία παρουσιάζουν λεπτομερώς τις πληροφορίες των πακέτων που διακινούνται σε ένα δίκτυο. Το εργαλείο tcpdump διαχειρίζεται και λειτουργεί μέσω τερματικού ενώ το wireshark μέσω γραφικού περιβάλλοντος.

Συγκέντρωση Πληροφοριών(nmap)



Συγκέντρωση Πληροφοριών(nmap)

```
root@kali:~# nmap -sM 192.168.13.205

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-12 14:57 EEST
Nmap scan report for 192.168.13.205
Host is up (0.22s latency).
All 1000 scanned ports on 192.168.13.205 are closed
MAC Address: 00:50:56:AF:3E:05 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.52 seconds
root@kali:~# iptables -vn -L
Chain INPUT (policy ACCEPT 5844 packets, 780K bytes)
 pkts bytes target     prot opt in     out     source               destination
 4118  166K ACCEPT     all  --  *      *       192.168.13.205       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 5674 packets, 701K bytes)
 pkts bytes target     prot opt in     out     source               destination
 7030  303K ACCEPT     all  --  *      *       0.0.0.0/0            192.168.13.205
```

Συγκέντρωση Πληροφοριών(nmap)

```
root@kali:~# nmap -sX 192.168.13.205

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-12 14:49 EEST
Nmap scan report for 192.168.13.205
Host is up (0.22s latency).
All 1000 scanned ports on 192.168.13.205 are closed
MAC Address: 00:50:56:AF:3E:05 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 33.65 seconds
root@kali:~# iptables -vn -L
Chain INPUT (policy ACCEPT 2806 packets, 368K bytes)
 pkts bytes target     prot opt in     out     source               destination
 2087 84381 ACCEPT     all  --  *      *       192.168.13.205       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2666 packets, 337K bytes)
 pkts bytes target     prot opt in     out     source               destination
 3065  144K ACCEPT     all  --  *      *       0.0.0.0/0            192.168.13.205
```

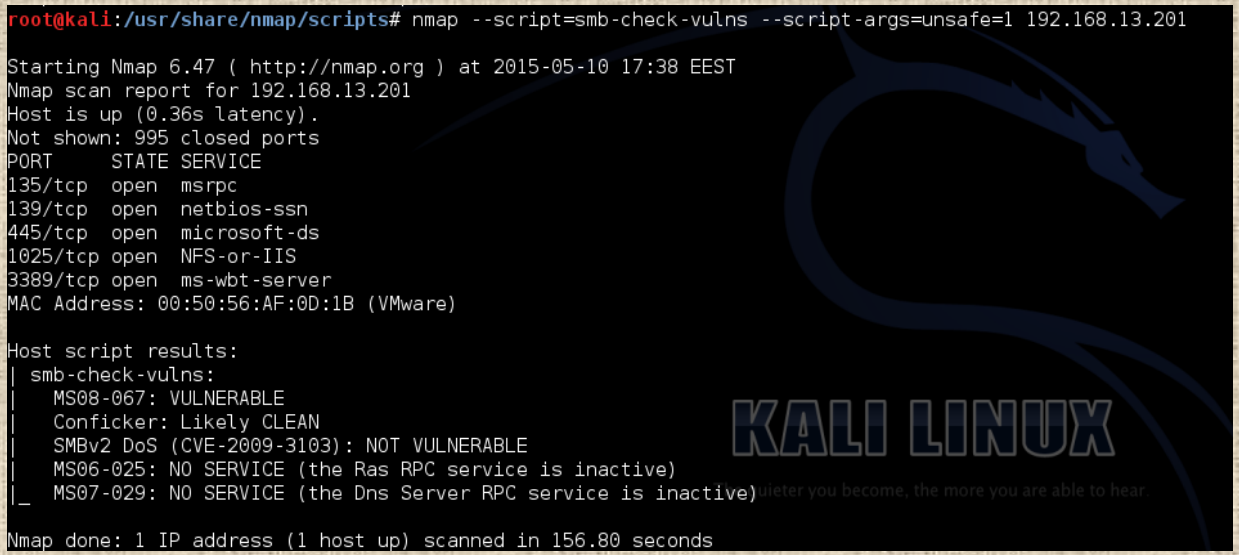
Συγκέντρωση Πληροφοριών(nmap)

```
root@kali:~# nmap -sA 192.168.13.205

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-12 14:55 EEST
Nmap scan report for 192.168.13.205
Host is up (0.22s latency).
All 1000 scanned ports on 192.168.13.205 are unfiltered
MAC Address: 00:50:56:AF:3E:05 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 33.18 seconds
root@kali:~# iptables -vn -L
Chain INPUT (policy ACCEPT 4567 packets, 619K bytes)
 pkts bytes target     prot opt in     out     source               destination
 3104  125K ACCEPT     all  --  *      *       192.168.13.205       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4224 packets, 528K bytes)
 pkts bytes target     prot opt in     out     source               destination
 5045  224K ACCEPT     all  --  *      *       0.0.0.0/0            192.168.13.205
```

Συγκέντρωση Πληροφοριών(nmap)

```
root@kali:~# nmap -sU 192.168.13.205

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-12 14:59 EEST
Nmap scan report for 192.168.13.205
Host is up (0.22s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
3456/udp open|filtered IISrpc-or-vat
MAC Address: 00:50:56:AF:3E:05 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 95.34 seconds
root@kali:~# iptables -vn -L
Chain INPUT (policy ACCEPT 7174 packets, 968K bytes)
 pkts bytes target     prot opt in     out     source               destination
 5124  223K ACCEPT     all  --  *      *       192.168.13.205       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 7112 packets, 854K bytes)
 pkts bytes target     prot opt in     out     source               destination
 8989  361K ACCEPT     all  --  *      *       0.0.0.0/0            192.168.13.205
```

Συγκέντρωση Πληροφοριών(nmap)



Υπολογιστικό Νέφος

- Το υπολογιστικό νέφος όπως ορίζεται από το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), αποτελεί ένα μοντέλο το οποίο καθιστά δυνατή την κατ'απαίτηση πρόσβαση μέσω ενός δικτύου σε μοιραζόμενους και διαρθρώσιμους πόρους οι οποίοι είναι σε θέση να γίνουν λειτουργικοί με ελάχιστη διαχείριση. Η τεχνολογία του υπολογιστικού νέφους χαρακτηρίζεται από πέντε στοιχεία:
  - Κατ΄απαίτηση αυτοεξυπηρέτηση
  - Ευρεία δικτυακή πρόσβαση
  - Ελαστικότητα
  - Διαθεσιμότητα
  - Κλιμακοθετησιμότητα

Υπολογιστικό Νέφος (συν.)

- Η διαθεσιμότητα είναι η ιδιότητα ενός συστήματος ή υπηρεσίας να παραμένει προσβάσιμο και χρηστικό στους τελικούς χρήστες χωρίς διακοπή. Επιπλέον, η διαθεσιμότητα αναφέρεται στην ικανότητα παροχής υπηρεσιών από ένα σύστημα ακόμα κι οταν τα υποσυστήματα αυτού αντιμετωπίζουν προβλήματα.

- Η κλιμακοθετησιμότητα είναι η ικανότητα των υπηρεσιών του υπολογιστικού νέφους να εξυπηρετούν τον φόρτο εργασίας κάθε χρονική στιγμή με το κατάλληλο πλήθος πόρων. Αυτό επιτυγχάνεται μέσω κλιμάκωσης των χρησιμοποιούμενων πόρων. Από την μεριά του πελάτη, η κλιμακοθετησιμότητα αντιλαμβάνεται ως η ικανότητα η οποία του παρέχεται να χρησιμοποιεί ένα μεγάλο πλήθος πόρων οι οποίοι του παρέχονται κατά δική του βούληση. Από την μεριά του παρόχου της υπηρεσίας υπολογιστικού νέφους, η κλιμακοθετησιμότητα είναι η υποχρέωση η οποία του έχει ανατεθεί για την ικανοποίηση των αναγκών των χρηστών χωρίς να δημιουργούνται περιορισμοί. Η κλιμακοθετησιμότητα ικανοποιείται με την διαδικασία εικονικοποίησης φυσικών πόρων.

Υπολογιστικό Νέφος (συν.)

- Η ελαστικότητα είναι η ικανότητα των υπηρεσιών του υπολογιστικού νέφους να προσαρμόζουν τους πόρους που χρησιμοποιούν στην κλιμακα του χρόνου σύμφωνα με το φόρτο εργασίας που τους ανατίθεται. Το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ορίζει την ελαστικότητα ως την ικανότητα που διαθέτουν οι πελάτες μιας υπηρεσίας να λαμβάνουν και να αποδεσμεύουν πόρους σύμφωνα με τις ανάγκες τους.

- Η κατ'απαίτηση αυτοεξυπηρέτηση αναφέρεται στη αυτόματη παροχή πόρων στον τελικό χρήστη χωρίς να είναι αναγκαία η επέμβαση φυσικού προσώπου ώστε να πραγματοποιηθεί.

- Η ευρεία δικτυακή πρόσβαση αναφέρεται στην δυνατότητα των υπηρεσίων να είναι διαθέσιμες στους τελικούς χρήστες μέσω του διαδικτύου ανεξάρτητα από το μέσο που χρησιμοποιείται και την γεωγραφική τοποθεσία.

Μοντέλα εξάπλωσης

- Δημόσιο(Public): Η υποδομή του παρόχου προβλέπεται για ανοιχτή χρήση, υπερέχει ως προς την κλιμακοθετησιμότητα, την απλότητα και το κόστος της παρεχόμενης υπηρεσίας. Το δημόσιο υπολογιστικό νέφος δεν παρέχει ικανοποιητικό επίπεδο ασφάλειας.

- Ιδιωτικό(Private): Η υποδομή του παρόχου προβλέπεται για αποκλειστική χρήση από έναν οργανισμό ή επιχείρηση και περιλαμβάνει περιορισμένο πλήθος χρηστών. Το επίπεδο ασφάλειας είναι υψηλό λόγω του τύπου δεδομένων που διαχειρίζεται.

- Κοινοτικό(Community): Η υποδομή του παρόχου προβλέπεται για αποκλειστική χρήση από από μια συγκεκριμένη κοινότητα ατόμων και τα χαρακτηριστικά του καθορίζονται από τις απαιτήσεις τους.

- Υβριδικό(hybrid): Η υποδομή του παρόχου αποτελεί σύνθεση τουλάχιστον δύο από τις παραπάνω υποδομές. Συνήθως χαρακτηρίζεται από την κλιμακοθετησιμότητα της δημόσιας υποδομής και από το επίπεδο ασφάλειας της ιδιωτικής.

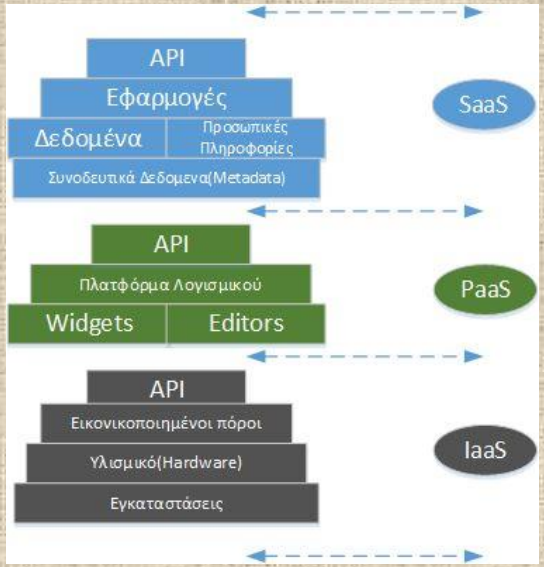
Μοντέλα υπηρεσιών

- SaaS: Η διανεμόμενη υπηρεσία είναι μια εφαρμογή της οποίας το λογισμικό λειτουργεί και στεγάζεται στην υποδομή του παρόχου. Οι τελικοί χρήστες δεν διαχειρίζονται την υπηρεσία και έχουν δυνατότητα επέμβασης στον τρόπο λειτουργίας της. Ο πάροχος είναι υπεύθυνος για την ασφάλεια της υπηρεσίας, ενώ ο χρήστης για τα δεδομένα που διαχειρίζεται κατά την χρήση της.

- PaaS: Η διανεμόμενη υπηρεσία είναι μια πλατφόρμα μέσω της οποίας οι τελικοί χρήστες έχουν την δυνατότητα έκθεσης δικής τους υπηρεσίας, η οποία χρησιμοποιεί τους πόρους της υποδομής του παρόχου. Η ευθύνη ως προς την ασφάλεια είναι μοιρασμένη στον χρήστη και στον πάροχο της υποδομής.

- IaaS: Η διανεμόμενη υπηρεσία είναι εικονικά συστήματα τα οποία χρησιμοποιούν εικονικοποιημένους πόρους της υποδομής του παρόχου. Η ευθύνη της ασφάλειας του εικονικού συστήματος ανατίθεται στον χρήστη και ο πάροχος είναι υπεύθυνος για την ασφάλεια του υλισμικού.

Μοντέλα υπηρεσιών (συν.)



Θέματα ασφάλειας στα μοντέλα υπηρεσιών

- Λόγω εξαρτήσεων μεταξύ των μοντέλων υπηρεσιών, οι απειλές που υφίστανται στο μοντέλο IaaS επαγωγικά υφίστανται και για τα υπόλοιπα μοντέλα υπηρεσιών.
- Στο μοντέλο SaaS, η ασφάλεια ως προς τον τρόπο διαχείρισης και αποθήκευσης των δεδομένων εξαρτάται από το μοντέλο εξάπλωσης του παρόχου. Έτσι, οι απειλές και οι κίνδυνοι που δημιουργούνται στο δημόσιο υπολογιστικό νέφος λόγω του μειωμένου επιπέδου ασφάλειας επηρεάζουν τα δεδομένα των χρηστών.
- Το μοντέλο PaaS αποτελείται από δύο επίπεδα ασφάλειας:
  - Το επίπεδο ασφάλειας της πλατφόρμας συγκραφής του πηγαίου κώδικα μιας εφαρμογής.
  - Το επίπεδο ασφάλειας των δεδομένων που διαχειρίζεται η εφαρμογή.

Θέματα ασφάλειας στα μοντέλα υπηρεσιών (συν.)

- Λόγω των εξαρτήσεων που υπάρχουν μεταξύ των μοντέλων υπηρεσιών και του τρόπου λειτουργίας του υπολογιστικού νέφους, κρίνεται απαραίτητο ο κάθε πάροχος υπηρεσιών να κατέχει υπο τον έλεγχό του και τα τρία μοντέλα. Με αυτόν τον τρόπο, ο πάροχος παρακολουθεί την λειτουργία τους και αντιμετωπίζει απειλές οι οποίες παρουσιάζονται σε κάθε ένα και επηρεάζουν τα υπόλοιπα κατά την παροχή των υπηρεσιών.

- Σε διαφορετική περίπτωση όπου τρείς πάροχοι συνεργάζονται για την παροχή των υπηρεσιών τότε θα παρουσιάζονταν περιορισμοί. Ο κάθε πάροχος θα είχε υπό τον έλεγχό του ένα από τα μοντέλα υπηρεσιών και σε περίπτωση που πραγματοποιηθεί επιτυχής επίθεση σε ένα εξ'αυτών τότε θα υπάρξουν συνέπειες σε όλα με αποτέλεσμα να μην υπάρχει διαφάνεια ως προς το ποιός είναι υπεύθυνος για την αδυναμία παροχής των προσδοκώμενου επιπέδου υπηρεσιών.

Εικονικοποίηση στο υπολογιστικό νέφος

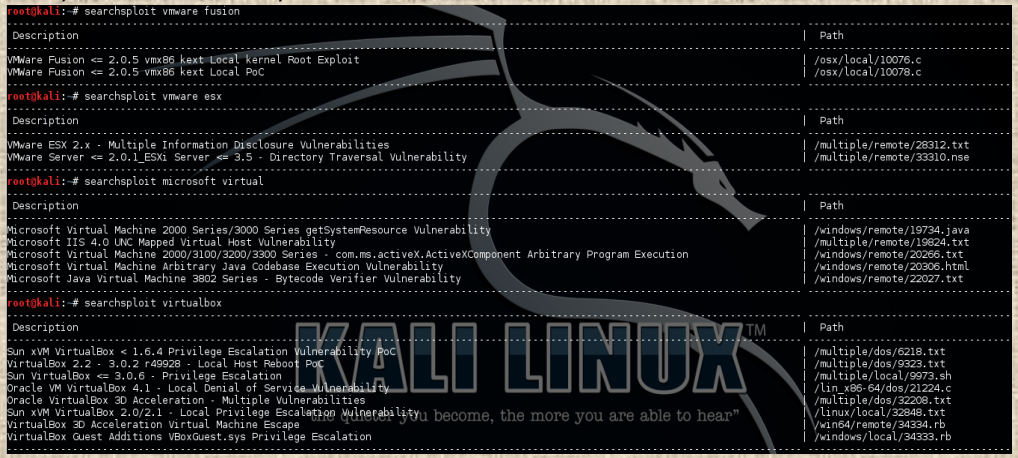
- Η διαδικασία εικονικοποίησης είναι απαραίτητη στο περιβάλλον υπολογιστικού νέφους εφόσον καταστεί εφικτή την εκτέλεση πολλαπλών εικονικών συστημάτων(VMs) ταυτόχρονα σε ένα φυσικό στοιχείο υλισμικού. Αυτή η διαδικασία λειτουργεί με μεγάλη ταχύτητα με αποτέλεσμα μέσω αυτής να βελτιώνεται η κλιμαθετησιμότητα. Η διαδικασία της εικονικοποίησης πραγματοποιείται από τους εικονικοποιητές οι οποίοι διαμοιράζουν τους φυσικούς πόρους στα φιλοξενούμενα συστήματα(guests).
- Ωστόσο, με την υιοθέτηση της διαδικασίας της εικονικοποίησης από τους παρόχους υπολογιστικού νέφους δημιουργούνται κίνδυνοι και απειλές για την ασφάλεια της υποδομής. Αυτό συμβαίνει επειδή το λογισμικό εικονικοποίησης προσθέτει ενα επιπλέον αφαιρετικό επίπεδο μεταξύ των λειτουργικών συστημάτων και του υλισμικού. Μέσω του περιβάλλοντος εικονικοποίησης είναι αδύνατη η απομόνωση ενος φιλοξενούμενου συστήματος από τα υπόλοιπα επειδή χρησιμοποιούν κοινό λογισμικό.

Κίνδυνοι και απειλές λόγω εικονικοποίησης

- Τα τρωτά σημεία ενός συστήματος εικονικοποίησης θα μπορούσαν να οδηγήσουν σε εκμετάλευση αυτού και κατά συνέπεια σε εκμετάλευση όλων των φιλοξενούμενων συστημάτων του.
- Το τρωτό σημείο με αναγνωριστικό CVE--2005-4459 επιτρέπει την απομακρυσμένη εκτέλεση κώδικα μέσω της υπερχείλησης του χώρου της σωρού που χρησιμοποιείται από το σύστημα εικονικοποίησης με συγκεκριμένες κακόβουλες αιτήσεις του πρωτοκόλλου File Transfer Protocol(FTP). Το τρωτό σημείο υπάρχει σε εκδόσεις των συστηματων εικονικοποίησης VMware ACE, VMware Gsx Server, VMware Player και VMware Workstation.
- Το τρωτό σημείο με αναγνωριστικό CVE-2015-3456 και κωδικό όνομα VENOM επιτρέπει την εκμετάλλευση του συστήματος εικονικοποίησης μέσω ενός σφάλματος του εικονικού εύκαμπτου δίσκου(floppy drive). Το τρωτό σημείο υπάρχει σε εκδόσεις των συστηματων εικονικοποίησης XEN, KVM και QEMU.

Κίνδυνοι και απειλές λόγω εικονικοποίησης (συν.)

- Αναγνωριστικά γνωστών τρωτών σημείων σε συστήματα εικονικοποίησης τα οποία χρησιμοποιούνται από παρόχους υπολογιστικού νέφους αποτελούν τα CVE-2007-1744, CVE-2008-0923, CVE-2009-1244, CVE-2012-0217 και CVE-2014-0983.



Κίνδυνοι και απειλές λόγω εικονικοποίησης (συν.)

- Σε περίπτωση που ένα εκ των εικονικών συστημάτων προσβληθεί από ιό ή σκουλήκι τότε τίθεται σε κίνδυνο η ασφάλεια όλων των εικονικών συστηματων τα οποία αλληλεπιδρούν με αυτό. Αυτό συμβαίνει λόγω της αρχιτεκτονικής του υπολογιστικού νέφους κατά την οποία για την παροχή μιας υπηρεσίας είναι αναγκαίο να αλληλεπιδρούν τα εικονικά συστήματα μεταξύ τους και λόγω του τύπου του κακόβουλου λογισμικού το οποίο προσπαθεί να διαδοθεί ή να μεταδώσει ένα αντίγραφο του εαυτού του σε άλλα συστήματα του δικτύου.

- Η αντιμετώπιση θα μπορούσε να καταστεί εύκολη εάν υπήρχε μόνο μια πύλη εισόδου/εξοδου δεδομένων από το ένα δίκτυο στο άλλο, ωστόσο στο υπολογιστικό νέφος διαφορετικά εικονικά συστήματα αλληλεπιδρούν με εικονικά συστήματα σε διαφορετικά δίκτυα.

Τύποι επιθέσεων μέσω εικονικοποίησης

- Επιθέσεις μέσω συστημάτων εικονικοποίησης στην υποδομή των παρόχων υπολογιστικού νέφους:
  - Αρνηση παροχής υπηρεσιών στο σύστημα εικονικοποίησης
  - Χρήση rootkit
  - Χρήση στιγμιότυπων

Τύποι επιθέσεων μέσω εικονικοποίησης (συν.)

- Η επίθεση άρνησης παροχής υπηρεσιών στο σύστημα εικονικοποίησης πραγματοποιείται κυρίως σε υπηρεσίες τύπου IaaS όπου οι χρήστες έχουν στην κατοχή τους εικονικά συστήματα με δυνατότητα διαχειρισής τους. Η συγκεκριμένη επίθεση έχει ως στόχο την εξάντληση των φυσικών πόρων του υλισμικού στοιχείου, οι οποίοι χρησιμοποιούνται απο το σύστημα εικονικοποίησης για την λειτουργία των φιλοξενούμενων εικονικών συστημάτων.

- Η επίθεση άρνησης παροχής υπηρεσιών μπορεί να πραγματοποιηθεί και διαμέσου μιας υπηρεσίας PaaS, με κώδικα ο οποίος μέσω της πλατφόρμας εξαντλεί τους παρεχόμενους πόρους και σε περίπτωση αποτυχίας της απομόνωσης των πόρων ενός χρήστη θα εξαντληθούν οι πόροι στο σύνολό τους.

Τύποι επιθέσεων μέσω εικονικοποίησης (συν.)

- Η επίθεση άρνησης παροχής υπηρεσιών στο σύστημα εικονικοποίησης πραγματοποιείται κυρίως σε υπηρεσίες τύπου IaaS όπου οι χρήστες έχουν στην κατοχή τους εικονικά συστήματα με δυνατότητα διαχειρισής τους. Η συγκεκριμένη επίθεση έχει ως στόχο την εξάντληση των φυσικών πόρων του υλισμικού στοιχείου, οι οποίοι χρησιμοποιούνται απο το σύστημα εικονικοποίησης για την λειτουργία των φιλοξενούμενων εικονικών συστημάτων.

- Η επίθεση άρνησης παροχής υπηρεσιών μπορεί να πραγματοποιηθεί και διαμέσου μιας υπηρεσίας PaaS, με κώδικα ο οποίος μέσω της πλατφόρμας εξαντλεί τους παρεχόμενους πόρους και σε περίπτωση αποτυχίας της απομόνωσης των πόρων ενός χρήστη θα εξαντληθούν οι πόροι στο σύνολό τους.

Τύποι επιθέσεων μέσω εικονικοποίησης (συν.)

- Σε περίπτωση που ένα rootkit παραβιάσει το σύστημα εικονικοποίησης τότε ο επιτιθέμενος αποκτά τον έλεγχο του στοιχείου του υλισμικού. Rootkit το οποίο χρησιμοποιείται επί του παρόντος και αποτελεί απειλή για την υποδομή του υπολογιστικού νέφους είναι το Blue Pill.
- Το Blue Pill είναι κακόβουλο λογισμικό βασισμένο στην εικονικοποίηση το οποίο μπορεί να χρησιμοποιηθεί εναντίον οποιουδήποτε συστήματος ανεξάρτητα από την αρχιτεκτονική του υλισμικού ή του εγκατεστημένου λειτουργικού συστήματος. Αφού πραγματοποιηθεί η εγκατάστασή του, λειτουργεί ως σύστημα εικονικοποίησης μεταξύ του αρχικού λειτουργικού συστήματος ή του αρχικού συστήματος εικονικοποίησης και του υλισμικού. Εφόσον λειτουργεί σε κατώτερο αφαιρετικό επίπεδο από το αρχικό σύστημα είναι σε θέση να το ελέγχει και κατά συνέπεια να ελέγχει τους πόρους τους οποίους διανέμει στα επιμέρους εικονικά συστήματα.
- Το Blue Pill είναι Proof of Concept έτσι για να πραγματοποιηθεί επιτυχής επίθεση είναι απαραίτητο ο επιτιθέμενος να έχει συγκεντρώσει πληροφορίες σχετικά με το λειτουργικό σύστημα και το σύστημα εικονικοποίησης το οποίο χρησιμοποιείται και να κατέχει υψηλό επίπεδο ικανοτήτων

Τύποι επιθέσεων μέσω εικονικοποίησης (συν.)

- Σε περίπτωση κατά την οποία εκτεθεί το σύστημα εικονικοποίησης, ο επιτιθέμενος έχει την δυνατότητα χρήσης παλαιότερων στιγμιότυπων.

- Επανεφέροντας τα εικονικά συστήματα σε μια παρελθοντική κατάσταση

  – Αποφεύγεται η εφαρμογή νέων πολιτικών και λογισμικού ασφάλειας για την προστασία πληροφοριών και δεδομένων τα οποία διαχειρίζονται.

  – Αποφεύγεται η εφαρμογή ενημερώσεων ασφαλείας οι οποίες “μπαλώνουν” τρωτά σημεία.

Δούρειοι ίπποι στο υπολογιστικό νέφος

- Οι εικόνες(images) στο υπολογιστικό νέφος είναι κρίσιμης σημασίας αφού αποτελούν την βάση για την λειτουργία των επιμέρους συστατικών μιας υπηρεσίας.
- Οι εικόνες κατασκευάζονται από τους εκδότες (publishers) και κατατίθονται στο αποθετήριο (repository) του υπολογιστικού νέφους από όπου διανέμονται για χρήση στους ανακτώντες (retrievers). Οι εκδότες είναι οι κατασκευαστές των εικονικών εικόνων και μπορεί να είναι διαχειριστές του υπολογιστικού νέφους ή χρήστες μιας IaaS υπηρεσίας. Οι ανακτώντες είναι χρήστες μια υπηρεσίας IaaS και χρησιμοποιούν τις εικονικές εικόνες για την δημιουργία instances διακομιστών(servers).
- Η εισαγωγή εικόνων στην υποδομή των παρόχων υπολογιστικού νέφους δημιουργεί ένα τρωτό σημείο το οποίο επιτρέπει στους επιτιθέμενους να χρησιμοποιούν τις εικόνες ως περιέκτη (container) δούρειων ίππων.

Δούρειοι ίπποι στο υπολογιστικό νέφος (συν.)

- Για να κατασκευάσουν οι εισβολείς δούρειους ίππους πρέπει να κατέχουν γνώση του λειτουργικού συστήματος και των εφαρμογών οι οποίες δραστηριοποιούνται σε αυτό ώστε να παραμετροποιήσουν κατάλληλα τις εξαρτήσεις ως προς το λογισμικό του δούρειου ίππου οι οποίες είναι αναγκαίες για την επιτυχή επίθεση.

- Έτσι, έχοντας την δυνατότητα οι εισβολείς να εισάγουν δικές τους εικόνες, πλέον δεν υπάρχει ανάγκη για συλλογή πληροφοριών πριν την εκμετάλλευση ενός εικονικού συστήματος αφού ο δούρειος ίππος έχει παραμετροποιηθεί ήδη στην εικόνα.

- Απαραίτητος λοιπόν είναι ο συνεχής έλεγχος των εικόνων οι οποίες κατατίθονται στο αποθετήριο για την ανίχνευση κακόβουλου λογισμικού.

Αντιμετώπιση απειλών στο υπολογιστικό νέφος

- Θα πρέπει να χρησιμοποιούνται συστήματα τα οποία θα πραγματοποιούν ανάλυση συμπεριφοράς(behavior analysis) και ανάλυση γνώσης(knowledge analysis).
- Τα συστήματα ανάλυσης συμπεριφοράς αναγνωρίζουν και καταγράφουν το προφίλ των ενεργειών και δραστηριοτήτων ενός χρήστη με αποτέλεσμα σε περίπτωση απόκλισης από αυτό το προφίλ να αναγνωρίζεται ο χρήστης ώς επιτιθέμενος και να λαμβάνονται τα κατάλληλα αντίμετρα.
- Τα συστήματα ανάλυσης γνώσης χρησιμοποιούν ένα έμπειρο σύστημα για να περιγράψουν κακόβουλη συμπεριφορά μέσω ενός κανόνα. Πλεονέκτημα αυτής της μεθόδου αποτελεί το γεγονός πως είναι εφικτό να συνυπάρξουν ταυτόχρονα πολλοί κανόνες. Το συγκεκριμένο σύστημα καταγράφει μια σειρά από ενέργειες και χρησιμοποιεί τους κανόνες για να ανιχνεύσει κακόβουλη συμπεριφορά.
- Κρίνεται απαραίτητο να τεθεί σε εφαρμογή ένα μοντέλο ανίχνευσης εισβολών το οποίο θα είναι κατανεμημένο όπως και η αρχιτεκτονική του υπολογιστικού νέφους σε περισσότερα σημεία τα οποία θα αλληλεπιδρούν.

Αντιμετώπιση απειλών στο υπολογιστικό νέφος (συν.)

- Κατανεμημένα συστήματα ανίχνευσης εισβολών αποτελούν τα : Grid Intrusion Detection Architecture, DCPortalsNg, SnortFlow και CyberGuarder.

- Το σύστημα DCPortalsNg προσφέρει απομόνωση στα εικονικά δίκτυα κάνοντας χρήση της τεχνολογίας δικτύων καθορισμένων από το λογισμικό(SDN).

- Το SnortFlow είναι ένα σύστημα αποτροπής εισβολών βασισμένο στα συστήματα Snort και OpenFlow. Σε αυτό η ύποπτη δραστηριότητα ανιχνεύεται και στην συνέχεια ειδοποιείται ένα υποσύστημα δημιουργίας κανόνων.

- Το σύστημα CyberGuarder προσφέρει τρείς υπηρεσίες για την διασφάλιση των εικονικών δικτύων, την υπηρεσία ασφάλειας των εικονικών συστημάτων, την υπηρεσία ασφάλειας των εικονικών δικτύων και την υπηρεσία διαχείρισης των πολιτικών οι οποίες έχουν τεθεί σε εφαρμογή.

Βιβλιογραφία

- Stallings W., (2006) *Cryptography and Network Security,* 4th edition, Pearson Education, Inc. pp.671-696
- Offensive Security, (2014) *Penetration Testing with Kali Linux,* Professional Information Security Training and Services, pp.13-371
- N. V. Database, *Common vulnerability scoring system ,* Available at: http://nvd.nist.gov/cvss.cfm
- CVE, *CVE Numbering Authorities,* The Standard for Information Security Vulnerability Names, Available at: www.cve.mitre.org/cve/can.html
- Fyodor, *Nmap,* Available at: https://nmap.org/
- Meiko J., Jorg S., Nils G., Luigi Lo I., "*On Technical Security Issues in Cloud Computing*", IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25, 2009

Βιβλιογραφία (συν.)

- Ms. Parag K. S., Ms. Sneha S., Dr. A. D. Gawande, (2012), "*Intrusion Detection System for Cloud Computing*", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.
- Kleber V., Alexandre S., Carlos W., Carla W., (2009), "*Intrusion Detection Techniques in Grid and Cloud Computing Environment*", IEEE Computer Society, August 26, 2009.
- Mazhar A., Samee U.K. and V. Vasilakos A. (2015). "*Security in cloud computing: Opportunities and challenges*", Information Sciences, Elsevier Journal, 2015.
- Mell P. and Grance T., (2011), "*The NIST Definition of Cloud Computing*", NIST, Special Publication 800-145
- Brona S., Jignesh V., 2012, "*A literature survey on virtualization security threats in cloud computing*", International Journal of Science and Research, 2012