Η αξία της έρευνας ευπαθειών στις δοκιμές παρείσδυσης

Δρ Πάτροκλος Αργυρούδης
argp@census.gr / Ερευνητής Ασφάλειας Η/Υ

census®

Λίγα λόγια για τη Census

- Παροχή εξειδικευμένων υπηρεσιών ασφάλειας Η/Υ που απαιτούν εργαστηριακό ή ερευνητικό έργο (lab work)
  - Penetration Testing
  - Code Auditing
  - Digital Forensics
  - Device / Software Vulnerability Research
  - Exploit Development
  - Training
  - κλπ.
- http://www.census.gr

Έρευνα

- Το ερευνητικό έργο εμπλουτίζει και διαμορφώνει τις υπηρεσίες
- Παρουσιάζεται σε διεθνή συνέδρια
  - Black Hat USA 2012
  - OWASP AppSec Research 2012
  - Black Hat Europe 2010 και 2011
  - AthCon 2010, 2011, 2012 και 2013
- Ενσωματώνεται σε εργαλεία του κλάδου
  - π.χ. Metasploit Framework
- Αποτελεί το ίδιο υπηρεσία

Έργο

- Παροχή υπηρεσιών σε διεθνές επίπεδο
  - Τράπεζες
  - Ασφαλιστικές
  - Εταιρείες ανάπτυξης λογισμικού
  - Πάροχοι διαδικτυακών υπηρεσιών
  - Κατασκευαστές δικτυακού ή άλλου εξοπλισμού
  - Integrators
  - Εταιρείες από το χώρο της ασφάλειας Η/Υ

Τι είναι η Έρευνα Ευπαθειών

- Vulnerability Research
- Στοχευμένη έρευνα σε
  - Εφαρμογές
  - Υπηρεσίες
  - Συσκευές
  - Πρωτόκολλα
  - Διαδικασίες
- Σκοπός: η εύρεση ευπαθειών ασφάλειας

Τι είναι η Έρευνα Ευπαθειών

- Φάση 1η - Εύρεση Ευπαθειών
  - Κατανόηση του στόχου
  - Ανάλυση "εις βάθος" για την εύρεση ευπαθειών
  - Αποτύπωση συνθηκών που οδηγούν στην ευπάθεια
  - Εξέταση επικινδυνότητας και δυνατότητας εκμετάλλευσης
  - Αποτύπωση των (υπο)συστημάτων που επηρεάζει η ευπάθεια

Τεχνικές Εύρεσης Ευπαθειών

- Εξέταση πηγαίου κώδικα
  - Στατική ανάλυση
  - Δυναμική ανάλυση (π.χ. taint analysis)
- Reverse engineering
  - Στατική ανάλυση
  - Δυναμική ανάλυση (π.χ. binary instrumentation)
- Fuzzing
- Functional testing

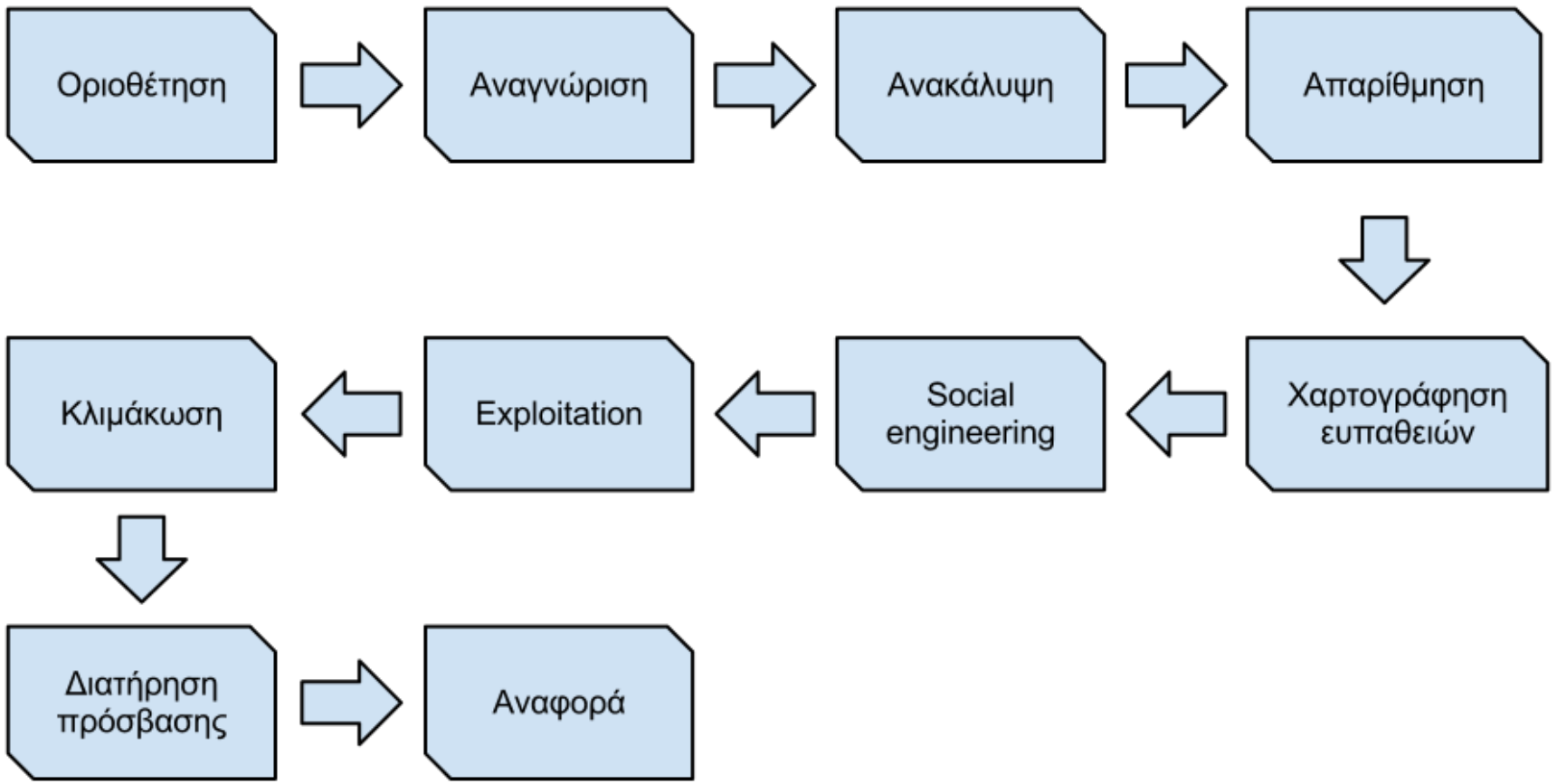
Τι είναι η Έρευνα Ευπαθειών

- Φάση 2η - Συγγραφή exploit
  - Συγγραφή ειδικού λογισμικού για την εκμετάλλευση της ευπάθειας (exploit)
  - Εργαλεία:
    - debuggers
    - encoders
    - λογισμικό για την εύρεση ROP gadgets
    - ...

Τι είναι η Έρευνα Ευπαθειών

- Φάση 3η - Ενημέρωση
  - Τεχνική αναφορά με προτεινόμενες διορθώσεις
  - Ενημέρωση κατασκευαστή
  - Ενημέρωση κοινού
    - Advisory & CVE όταν το επιτρέπει ο κατασκευαστής
  - Χρήση βοηθητικής πληροφορίας
    - καθιερωμένοι τύποι σφαλμάτων
    - πεδίο χρήσης του ευπαθούς λογισμικού

Πώς γίνονται σήμερα οι δοκιμές παρείσδυσης



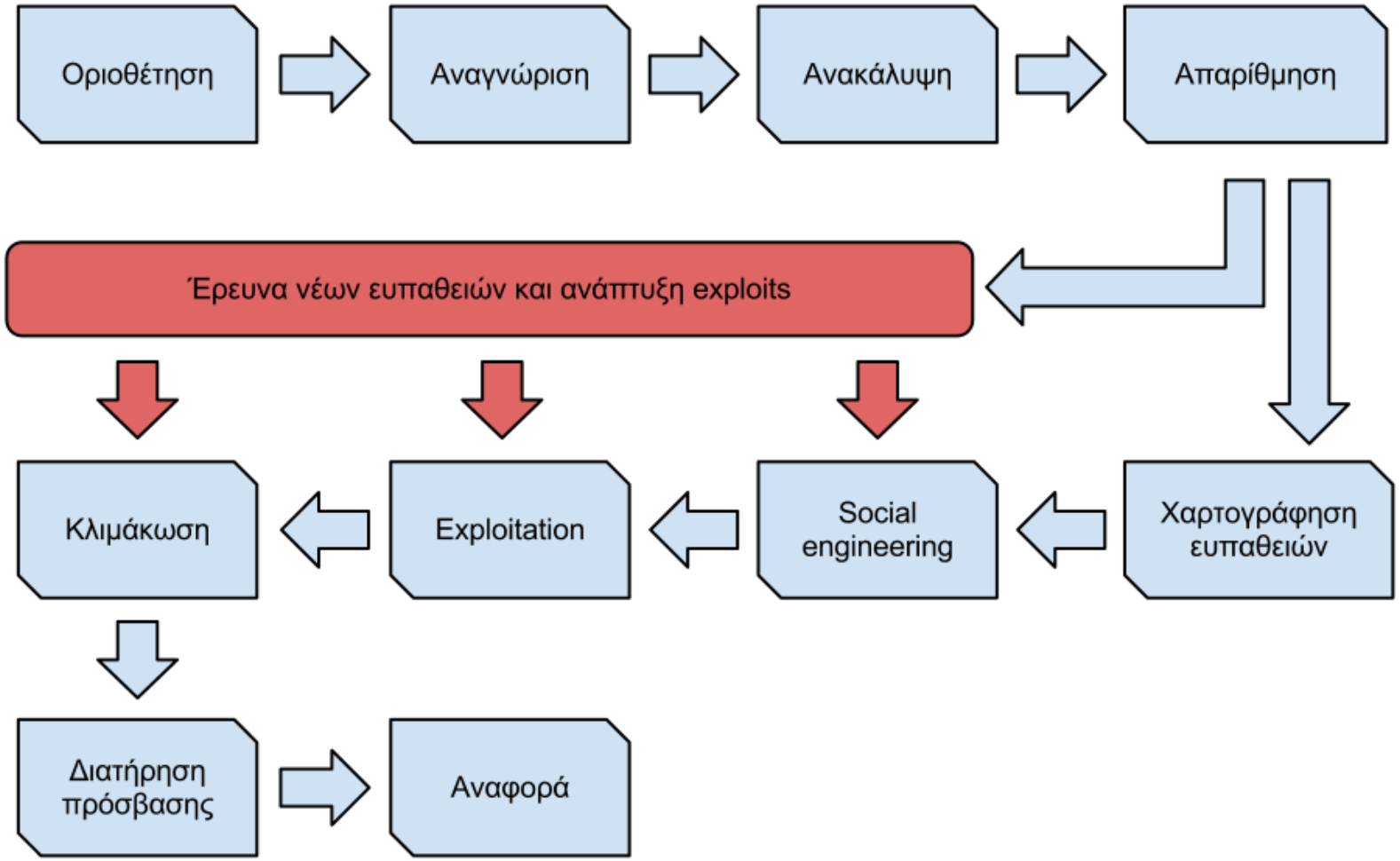
Πώς γίνονται σήμερα οι δοκιμές παρείσδυσης

- Εύρεση ευπαθειών μέσω αυτοματοποιημένων εργαλείων
  - Εσφαλμένη απεικόνιση της πραγματικής επιφάνειας ευπαθειών
- Το ενημερωμένο λογισμικό θεωρείται ασφαλές
  - Οι υποδομές είναι ευάλωτες όταν στηρίζονται σε κακής ποιότητας ή/και λάθος ρυθμισμένο λογισμικό
  - Τα 0-day exploits και οι στοχευμένες επιθέσεις αποτελούν καθημερινή απειλή

Πώς γίνονται σήμερα οι δοκιμές παρείσδυσης

- Δίνεται ιδιαίτερη έμφαση στις client-side επιθέσεις
  - Δεν αφιερώνεται ο απαραίτητος χρόνος ώστε να εξεταστούν και άλλα μονοπάτια επίθεσης που είναι εξίσου σημαντικά

Πώς αλλάζει μια δοκιμή παρείσδυσης η έρευνα ευπαθειών



Πώς αλλάζει μια δοκιμή παρείσδυσης η έρευνα ευπαθειών

- Η ερευνητική ομάδα λειτουργεί παράλληλα με την ομάδα δοκιμών παρείσδυσης
- Εντοπίζει νέες αδυναμίες σε λογισμικό ή συστήματα που έχουν χαρακτηριστεί ως ενδιαφέροντα
- Τροφοδοτεί την ομάδα δοκιμών παρείσδυσης με νέα εργαλεία και exploits για συγκεκριμένες αδυναμίες

Πώς αλλάζει μια δοκιμή παρείσδυσης η έρευνα ευπαθειών

- Έτσι η δοκιμή παρείσδυσης μπορεί πλέον να εξετάσει και:
  - το σενάριο στοχευμένης επίθεσης
  - το σενάριο εκμετάλλευσης αδυναμίας με 0-day exploits
  - την ορθή λειτουργία των proactive μηχανισμών ασφάλειας
  - την ετοιμότητα απέναντι σε μια αγνώστου φύσης απειλή

Case study #1: Ευπάθεια εφαρμογής ιστού

- Στα πλαίσια ελέγχου παρείσδυσης εντοπίζεται σφάλμα τύπου SQL injection σε σύστημα CMS
- Κατά τη διερεύνηση προκύπτει ότι το σφάλμα είναι κοινό σε όλες τις εγκαταστάσεις του εν λόγω CMS
- Δημιουργείται το proof-of-concept exploit
- Γίνεται επιτυχημένη χρήση του exploit
- Ανακοινώνεται η ευπάθεια στην εταιρεία-δημιουργό του CMS
- 1 μήνα αργότερα ανακοινώνεται δημόσια η ευπάθεια και η εταιρεία-δημιουργός παρέχει νέα έκδοση του λογισμικού στους πελάτες της

Πώς βοήθησε η έρευνα ευπαθειών τον πελάτη

- Διαπιστώθηκε και διορθώθηκε η ευπάθεια (για όλους τους χρήστες του CMS)
- Η εκμετάλλευση της ευπάθειας επέτρεψε την πρόσβαση σε περαιτέρω συστήματα
- Ο πελάτης επανεξέτασε την επικινδυνότητα του ιστότοπου και τον κομβικό του χαρακτήρα
- Εφαρμόστηκαν νέα proactive μέτρα ασφάλειας
- Έγινε σαφής η ανάγκη διατήρησης του συμβολαίου συντήρησης με την εταιρεία-δημιουργό

Case study #2: Ευπάθεια διακομιστή αρχείων

- Στα πλαίσια ελέγχου παρείσδυσης η ομάδα λαμβάνει πρόσβαση σε διακομιστή αρχείων
- Υπάρχει πρόσβαση τύπου απλού χρήστη και απαιτείται πρόσβαση τύπου διαχειριστή
- Η ερευνητική ομάδα εξετάζει τον πυρήνα του λειτουργικού συστήματος και διαπιστώνει ότι είναι ευάλωτος σε γνωστό πρόβλημα ασφάλειας

Case study #2: Ευπάθεια διακομιστή αρχείων

- Η ομάδα έρευνας ετοιμάζει το κατάλληλο exploit
- Η ομάδα παρείσδυσης λαμβάνει την άδεια του τεχνικού υπευθύνου για να εκτελέσει το exploit
- Η εκτέλεση είναι επιτυχής
- Η ομάδα παρείσδυσης λαμβάνει προνόμια διαχειριστή στον εξυπηρετητή

Πώς βοήθησε η έρευνα ευπαθειών τον πελάτη

- Έγινε σαφές ότι οι αναβαθμίσεις ασφάλειας θα πρέπει να γίνονται και στις κρίσιμες υποδομές
- Δημιουργήθηκε διαδικασία αναβάθμισης κρίσιμων υποδομών
- Τα προνόμια διαχειριστή επέτρεψαν τον εντοπισμό και άλλων προβλημάτων όπως:
  - χρήση κοινών συνθηματικών μεταξύ υπηρεσιών
  - χρήση μη ασφαλών πρωτοκόλλων επικοινωνίας

Συμπεράσματα

- Παραδοσιακές δοκιμές παρείσδυσης
  - Με αυτοματοποιημένα εργαλεία, δίχως να εξετάζονται οι ευπάθειες και οι επιπτώσεις τους
  - Με ιδιαίτερο βάρος στα client-side attacks ώστε να παρουσιάζονται ως επιτυχημένες
  - Εσφαλμένη απεικόνιση της πραγματικής επιφάνειας ευπαθειών
- Δοκιμές παρείσδυσης με βάρος στην έρευνα ευπαθειών
  - Μεθοδολογία της Census
  - Ρεαλιστική εικόνα της ασφάλειας στο σύγχρονο περιβάλλον των στοχευμένων επιθέσεων

Ερωτήσεις