CSP010_W_H

Θέμα: Εισαγωγή στις δοκιμές διείσδυσης στην κυβερνοασφάλεια

ΕΚΠΑΙΔΕΥΤΕΣ:

Paresh Rathod (Laurea)

Christos Grigoriadis (Focal Point)
Ricardo Lugo (TALTECH)
Kitty Kioskli (Trustilio BV,)

ΠΑΡΟΥΣΙΑΣΗ ΑΠΌ:

Paresh Rathod

Πανεπιστήμιο Εφαρμοσμένων Επιστημών Laurea, Φινλανδία

Επισήμανση

- Χρηματοδοτημένο από την Ευρωπαϊκή Ένωση. Ωστόσο, οι απόψεις και οι γνώμες που εκφράζονται είναι αποκλειστικά του/των συγγραφέα/ων και δεν αντανακλούν κατ' ανάγκη της Ευρωπαϊκής Ένωσης ή της HADEA. Καμία εκ των Ευρωπαϊκής Ένωσης ή της χορηγούσας αρχής μπορούν να θεωρηθούν υπεύθυνοι γι' αυτές.
- Συμφωνία έργου αριθ. 101083594

Εισαγωγή στις δοκιμές διείσδυσης στην κυβερνοασφάλεια

- Εξερευνήστε τον κρίσιμο ρόλο των δοκιμών διείσδυσης στη διαφύλαξη των ψηφιακών περιουσιακών στοιχείων. Μάθετε πώς οι ηθικοί χάκερς αποκαλύπτουν μεθοδικά τις ευπάθειες για να ενισχύσουν τη στάση κυβερνοασφάλειας μιας οργάνωσης και να αποτρέψουν δαπανηρές παραβιάσεις δεδομένων

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

CyberSecPro

Κατανόηση του τοπίου της κυβερνοασφάλειας

- Το τοπίο της κυβερνοασφάλειας είναι σύνθετο και εξελίσσεται συνεχώς, με νέες απειλές και ευπάθειες να αναδύονται συνεχώς. Οι επιχειρήσεις αντιμετωπίζουν έντονη πρόκληση όσον αφορά τη διαφύλαξη των ψηφιακών τους περιουσιακών στοιχείων από εξελιγμένες επιθέσεις στον κυβερνοχώρο. Οι δοκιμές διείσδυσης είναι ένα κρίσιμο εργαλείο για τους οργανισμούς ώστε να αξιολογούν προληπτικά τη θέση ασφαλείας τους και να εντοπίζουν τις αδυναμίες τους πριν από την εκμετάλλευση ευπάθειας.

Ορίζοντας τις δοκιμές διείσδυσης

- Οι δοκιμές διείσδυσης, γνωστές και ως **ηθικό χάκινγκ, είναι** μια πρακτική προσομοίωσης επιθέσεων στον κυβερνοχώρο για να αποκτηθεί πρόσβαση στις άμυνες ενός οργανισμού.
- Στόχος είναι ο συστηματικός εντοπισμός και η εκμετάλλευση των ευπαθειών στα συστήματα, τα δίκτυα και τις εφαρμογές μιας οργάνωσης για την αξιολόγηση της συνολικής κατάστασης ασφαλείας
- Όσοι κάνουν δοκιμές διείσδυσης ενεργούν ως **έμπιστοι, εξουσιοδοτημένοι αντίπαλοι για** να αποκαλύψουν αδυναμίες που θα μπορούσαν να εκμεταλλευτούν από κακόβουλους φορείς, επιτρέποντας στις οργανώσεις να ενισχύσουν τα μέτρα κυβερνοασφάλειάς τους

Αρχές ηθικής παράκαμψης ασφαλείας

Εξουσιοδότηση χρήστη

Οι δοκιμές διείσδυσης εργάζονται με ρητή άδεια και εξουσιοδότηση χρήστη από την οργανωτική μονάδα που δοκιμάζεται, διασφαλίζοντας ότι παραμένουν εντός νομικών και ηθικών ορίων.

Πλήρης αποκάλυψη

Οι δοκιμαστές διείσδυσης παρέχουν ολοκληρωμένη, διαφανή αναφορά σχετικά με τις ευπάθειες που ανακαλύφθηκαν και τα βήματα που έγιναν για την εκμετάλλευσή τους

Ελαχιστοποίηση της βλάβης

Οι ηθικοί χάκερ θέτουν ως προτεραιότητα την ελαχιστοποίηση κάθε δυνητικής διακοπής ή ζημίας στα συστήματα κατά τη διάρκεια της διαδικασίας δοκιμών.

Συνεχής βελτίωση

Η ηθική παράκαμψη ασφαλείας είναι μια επαναληπτική διαδικασία, με στόχο τη συνεχή βελτίωση της κατάστασης ασφαλείας μιας οργάνωσης με την πάροδο του χρόνου.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Τύποι δοκιμών διείσδυσης

- **Δοκιμές διείσδυσης στο δίκτυο:** Αξιολόγηση της ασφάλειας της εσωτερικής και εξωτερικής δικτυακής υποδομής μιας οργάνωσης, συμπεριλαμβανομένων των διακομιστών, των τειχών (ηλεκτρονικής) προστασίας και των ασύρματων δικτύων.

- **Δοκιμές διείσδυσης σε εφαρμογές ιστού**: εντοπίζοντας αδυναμίες σε εφαρμογές δικτύου όπως έγχυση SQL, cross-site (XSS) και άλλες απειλές του OWASP Top 10.

- **Δοκιμές διείσδυσης σε κινητές εφαρμογές:** Εκτιμά την ασφάλεια των εφαρμογών για κινητά και τις αλληλεπιδράσεις τους με βάσεις δεδομένων, δίνοντας έμφαση στη διαρροή δεδομένων, στην μη ασφαλή ταυτοποίηση χρήστη και σε άλλες ευπάθειες που σχετίζονται με κινητά τηλέφωνα.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Αναγνώριση και συλλογή πληροφοριών

1

Πληροφορίες ανοικτού κώδικα (OSINT)

Συγκεντρώστε δημόσια διαθέσιμες πληροφορίες σχετικά με τον οργανισμό από ιστοσελίδες, κοινωνικής και διαδικτυακές πηγές για να αποκτήσετε μια ολοκληρωμένη εικόνα των συστημάτων, της υποδομής και των δυνητικών ευπαθειών του.

2

Σάρωση δικτύου και θυρών

Διεξάγετε σε βάθος σαρώσεις του δικτύου και των συστημάτων του στόχου για τον εντοπισμό ενεργών κεντρικών υπολογιστών, ανοικτών θυρών και δυνητικά ευάλωτων υπηρεσιών, θέτοντας τις βάσεις για τα επόμενα στάδια της δοκιμής διείσδυσης.

3

Εντοπισμός ευπάθειας

Αξιοποίηση εξειδικευμένων εργαλείων και πληροφοριών σχετικά με τις απειλές για τον συστηματικό εντοπισμό γνωστών ευπαθειών, λανθασμένων ρυθμίσεων και αδυναμιών στα συστήματα και τις εφαρμογές του στόχου που θα μπορούσαν να εκμεταλλευτούν κατά τη διάρκεια της δοκιμής διείσδυσης.

Εντοπισμός ευπάθειας και Ανάλυση

Συστηματική προσέγγιση

Οι δοκιμαστές διείσδυσης ακολουθούν μια δομημένη μεθοδολογία για να εντοπίσουν συστηματικά τις ευπάθειες στα συστήματα, τα δίκτυα και τις εφαρμογές του στόχου. Αυτό περιλαμβάνει τη χρήση εξειδικευμένων εργαλείων και τεχνικών για την αποκάλυψη των αδυναμιών.

Σάρωση Ευπαθειών

Χρησιμοποιούνται αυτοματοποιημένα εργαλεία σάρωσης ευπαθειών για τη σάρωση του στοχευμένου περιβάλλοντος για γνωστές ευπάθειες, λανθασμένες ρυθμίσεις και δυνητικά σημεία εισόδου που θα μπορούσαν να εκμεταλλευτούν από επιτιθέμενους.

Χειροκίνητη επαλήθευση

Οι δοκιμαστές διείσδυσης επαληθεύουν και επικυρώνουν επίσης χειροκίνητα τα εντοπισμένα τρωτά σημεία, διασφαλίζοντας την ακρίβεια των ευρημάτων και αποκτώντας βαθύτερη κατανόηση του δυνητικού αντίκτυπου και της δυνατότητας εκμετάλλευσης ευπάθειας.

Αξιολόγηση κινδύνου

Αφού εντοπιστούν οι ευπάθειες, οι ελεγκτές διείσδυσης αξιολογούν τον κίνδυνο που ενέχουν για την οργάνωση, λαμβάνοντας υπόψη παράγοντες όπως η πιθανότητα εκμετάλλευσης ευπάθειας και ο δυνητικός αντίκτυπος μιας επιτυχημένης επίθεσης.

Τεχνικές εκμετάλλευσης ευπάθειας

Εκμετάλλευση ευπάθειας

Εκμεταλλευτείτε τις εντοπισμένες Ευπάθειες για να αποκτήσετε μη εξουσιοδοτημένη πρόσβαση σε συστήματα, δίκτυα ή εφαρμογές.

Προγραμματισμός εκμετάλλευσης ευπάθειας

Ανάπτυξη λογισμικού εκμετάλλευσης για τον αυτοματισμό της εκμετάλλευσης των ευπαθειών που ανακαλύφθηκαν για βαθύτερη πρόσβαση.

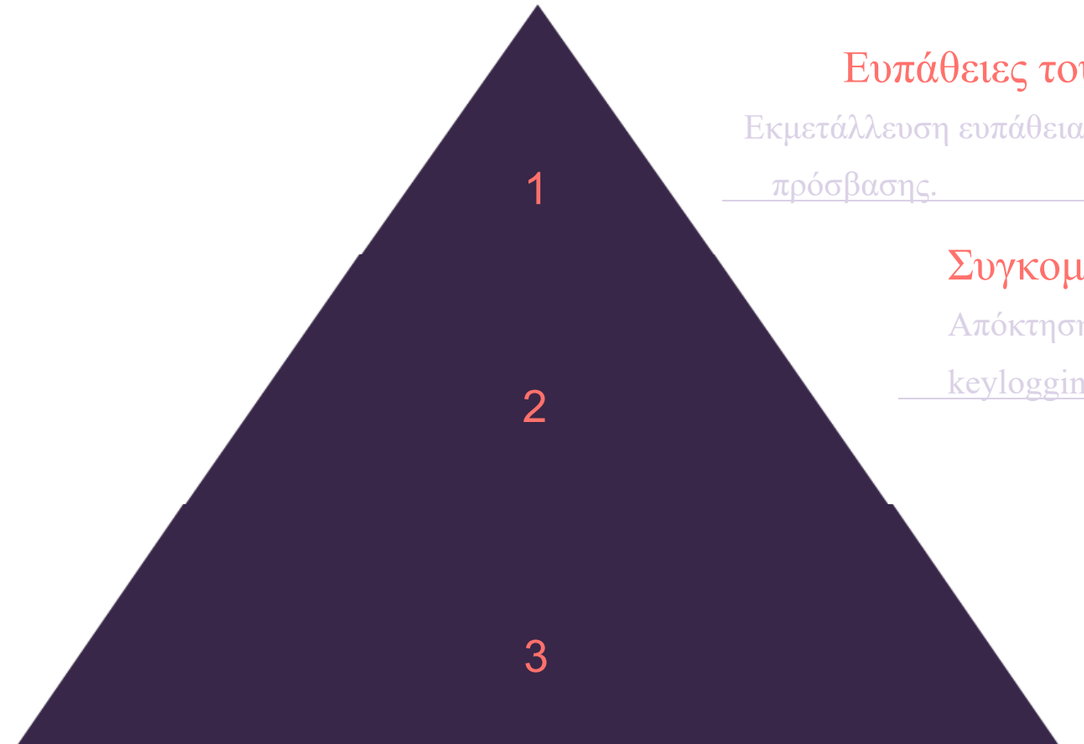
Κλιμάκωση προνομίων

Αυξήστε τα προνόμια των χρηστών για να αποκτήσετε ανώτερα επίπεδα πρόσβασης και ελέγχου στο περιβάλλον-στόχο.

Συντήρηση της πρόσβασης

Υλοποίηση κρυφών πρόσβασης σε συστήματα και άλλων τεχνικών για τη διατήρηση μακροπρόθεσμης πρόσβασης στα παραβιασμένα συστήματα.

Στρατηγικές κλιμάκωσης προνομίων



Ευπάθειες του συστήματος

Εκμετάλλευση ευπάθειας λογισμικού και λανθασμένων ρυθμίσεων για την απόκτηση αυξημένης πρόσβασης.

Συγκομιδή διαπιστευτηρίων

Απόκτηση διαπιστευτηρίων διαχειριστή μέσω phishing, keylogging, ή άλλα μέσα

Κατάχρηση υπηρεσιών (Service Hijacking)

Εκμεταλλευτείτε λανθασμένα ρυθμισμένες υπηρεσίες για να εκτελέσετε εντολές με ανώτερα προνόμια.

CSP010_W_H:

Η κλιμάκωση προνομίων είναι κρίσιμο βήμα στη δοκιμή διείσδυσης, επιτρέποντας στον ηθικό χάκερ να αποκτήσει αυξημένη πρόσβαση και έλεγχο στο σύστημα. Με τον συστηματικό εντοπισμό και την εκμετάλλευση ευπαθειών, την απόκτηση διαπιστευτηρίων υψηλού επιπέδου και προνομιακών υπηρεσιών ο δοκιμαστής διείσδυσης μπορεί να προχωρήσει βαθύτερα στο δίκτυο και να αποκτήσει πρόσβαση σε ευαίσθητους πόρους

Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Πλευρική (lateral) κίνηση και επιμονή

1

Κλιμάκωση προνομίων

Χρησιμοποιήστε την αυξημένη πρόσβαση που αποκτήσατε μέσω τεχνικών κλιμάκωσης προνομίων για να κινηθείτε πλευρικά στο δίκτυο.

2

Αξιοποίηση των σχέσεων εμπιστοσύνης

Εκμετάλλευση συνδέσεων εμπιστοσύνης μεταξύ συστημάτων και λογαριασμών για να αποκτήσετε πρόσβαση σε πρόσθετους πόρους και δεδομένα.

3

Καθιέρωση επιμονής

Υλοποίηση κρυφών πρόσβασης σε συστήματα, προγραμματισμένων διεργασιών και μηχανισμών για τη διατήρηση μακροπρόθεσμης πρόσβασης στα παραβιασμένα συστήματα.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Διατήρηση της πρόσβασης και κάλυψη των ιχνών

1

Μηχανισμοί επιμονής

Υλοποίηση κρυφών προσβάσεων σε συστήματα, προγραμματισμένων διεργασιών και άλλων τεχνικών για τη συντήρηση μακροπρόθεσμης πρόσβασης στα παραβιασμένα συστήματα, ακόμη και μετά την αρχική εκμετάλλευση ευπάθειας.

3

Απόκρυψη και μυστικότητα

Χρησιμοποιήστε τεχνικές όπως το process hollowing, η έγχυση

Κάλυψη ιχνών

Διαγράψτε προσεκτικά τα αρχεία καταγραφής, διαγράψτε το ιστορικό του προγράμματος περιήγησης και αφαιρέστε άλλα αποδεικτικά στοιχεία των δραστηριοτήτων δοκιμής διείσδυσης για να αποφύγετε τον εντοπισμό από τις ομάδες ασφαλείας.

κώδικα προγραμματισμού και το κακόβουλο λογισμικό χωρίς αρχεία για να αναμειχθείτε με την κανονική δραστηριότητα του συστήματος και την ενεργοποίηση συναγερμών ασφαλείας.

Διαρροή και κλοπή δεδομένων

Εξάγετε με ασφάλεια ευαίσθητα δεδομένα από το περιβάλλον, αξιοποιώντας την κρυπτογράφηση και άλλες μεθόδους για την αποφυγή εντοπισμού κατά τη διαδικασία μεταφοράς δεδομένων.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Αναφορά και καταγραφή

Η τελική φάση της διαδικασίας δοκιμής διείσδυσης περιλαμβάνει ολοκληρωμένη αναφορά και λεπτομερή καταγραφή. Οι δοκιμαστές διείσδυσης τεκμηριώνουν σχολαστικά τις δραστηριότητές τους, τα ευρήματα και τις συστάσεις τους, ώστε να παρέχουν σαφή κατανόηση της κατάστασης ασφαλείας του οργανισμού

Εξαρτήματα αναφοράς	Λεπτομερείς περιγραφές της μεθοδολογίας δοκιμών, των ευπαθειών που ανακαλύφθηκαν και των δυνητικών επιπτώσεων στην οργάνωση.
Λεπτομέρειες Ευπάθειας	Εις βάθος ανάλυση κάθε ευπάθειας, συμπεριλαμβανομένου του κινδύνου,
Καθοδήγηση αποκατάστασης	Συστάσεις με προτεραιότητα για την αντιμετώπιση των ευπαθειών που εντοπίστηκαν και την ενίσχυση της συνολικής ασφάλειας της οργάνωσης
Συνοπτική παρουσίαση	Μια υψηλού επιπέδου επισκόπηση της δέσμευσης για τις δοκιμές διείσδυσης, επισημαίνοντας τα βασικά ευρήματα και τις συστάσεις για εκτελεστικού επιπέδου ενδιαφερόμενους

Ευπάθεια έναντι δοκιμών διείσδυσης

Η αξιολόγηση ευπάθειας και οι δοκιμές διείσδυσης είναι και οι δύο ουσιώδη εξαρτήματα μιας ολοκληρωμένης στρατηγικής για την ασφάλεια στον κυβερνοχώρο, αλλά εξυπηρετούν διαφορετικούς σκοπούς.

Η αξιολόγηση ευπάθειας επικεντρώνεται στον εντοπισμό και την καταγραφή δυνητικών αδυναμιών στα συστήματα, τα δίκτυα και τις εφαρμογές μιας οργάνωσης. Παρέχει μια ολοκληρωμένη επισκόπηση της κατάστασης ασφαλείας.

Οι δοκιμές διείσδυσης, από την άλλη πλευρά, περιλαμβάνουν την ενεργή εκμετάλλευση των εντοπισμένων ευπαθειών για την αξιολόγηση του πραγματικού αντίκτυπου και του κινδύνου που ενέχουν για την οργάνωση. Προσομοιώνει τις τακτικές και τις τεχνικές ενός κακόβουλου επιτιθέμενου.

Μεθοδολογίες δοκιμών διείσδυσης

1

Σχεδιασμός

Καθορίστε το πεδίο εφαρμογής και τους κανόνες εμπλοκής.

2

Συλλογή πληροφοριών

Διεξαγωγή αναγνώρισης και ανακάλυψη ευπαθειών του συστήματος.

3

Εκμετάλλευση ευπάθειας

Εκμεταλλευτείτε τις ευπάθειες για να αποκτήσετε πρόσβαση και έλεγχο.

4

Μετά την εκμετάλλευση ευπάθειας

Συντήρηση της πρόσβασης, κλιμάκωση των προνομίων και διαρροή δεδομένων.

Οι μεθοδολογίες δοκιμών διείσδυσης ακολουθούν δομημένη προσέγγιση για την αξιολόγηση της κατάστασης ασφαλείας μιας οργάνωσης. Αυτό περιλαμβάνει προσεκτικό σχεδιασμό, ολοκληρωμένη συλλογή πληροφοριών, στοχευμένη εκμετάλλευση ευπαθειών και δραστηριότητες μετά την εκμετάλλευση την αξιολόγηση των επιπτώσεων των δυνητικών επιθέσεων στον πραγματικό κόσμο.

Κύκλος ζωής δοκιμών διείσδυσης

Σχεδιασμός

Καθορισμός σαφών στόχων, εφαρμογής και κανόνες εμπλοκής

1

2

Ευπάθεια

Συστηματική σάρωση και ανάλυση των συστημάτων για την αποκάλυψη αδυναμιών ασφαλείας.

3

4

Μετά την εκμετάλλευση ευπάθειας

Συντήρηση μόνιμης πρόσβασης, κλιμάκωση προνομίων και εξερεύνηση του παραβιασμένου δικτύου για

5

ευαίσθητες πληροφορίες.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Συλλογή πληροφοριών

Διεξαγωγή αναγνώρισης για τη συλλογή πληροφοριών σχετικά με το περιβάλλον του στόχου και τον εντοπισμό δυνητικών ευπαθειών.

Εκμετάλλευση ευπάθειας

Αξιοποίηση των ευπαθειών που ανακαλύφθηκαν για να αποκτήσουν ανεξουσιοδότητη πρόσβαση και έλεγχο στα συστήματα.

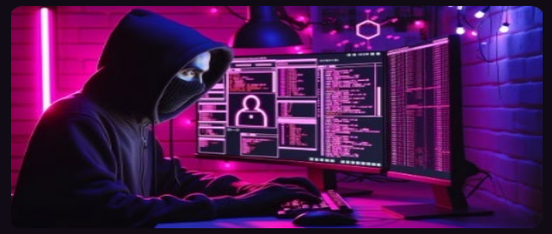
Αναφορά

Τεκμηριώνετε διεξοδικά ολόκληρη τη διαδικασία δοκιμής διείσδυσης και παρέχετε λεπτομερή ευρήματα και συστάσεις.

Εργαλεία και τεχνικές για δοκιμές διείσδυσης

Kali Linux

Μια δημοφιλής διανομή Linux που έχει σχεδιαστεί ειδικά για δοκιμές διείσδυσης, παρέχοντας μια ολοκληρωμένη σουίτα εργαλείων για σάρωση δικτύου, ανάλυση ευπαθειών και ανάπτυξη εκμεταλλεύσεων ευπάθειας.



Metasploit

Ένα ευέλικτο και ευρέως χρησιμοποιούμενο πλαίσιο λογισμικού δοκιμών διείσδυσης που απλοποιεί τη διαδικασία εντοπισμού, εκμετάλλευσης και αναφοράς ευπαθειών ασφαλείας σε συστήματα.

Burp Suite

Μια ολοκληρωμένη συλλογή δοκιμών ασφαλείας εφαρμογών ιστού που επιτρέπει στους ελεγκτές διείσδυσης να υποκλέπτουν, να αναλύουν και να χειρίζονται την κίνηση του ιστού για να εντοπίζουν και να εκμεταλλεύονται ευπάθειες.

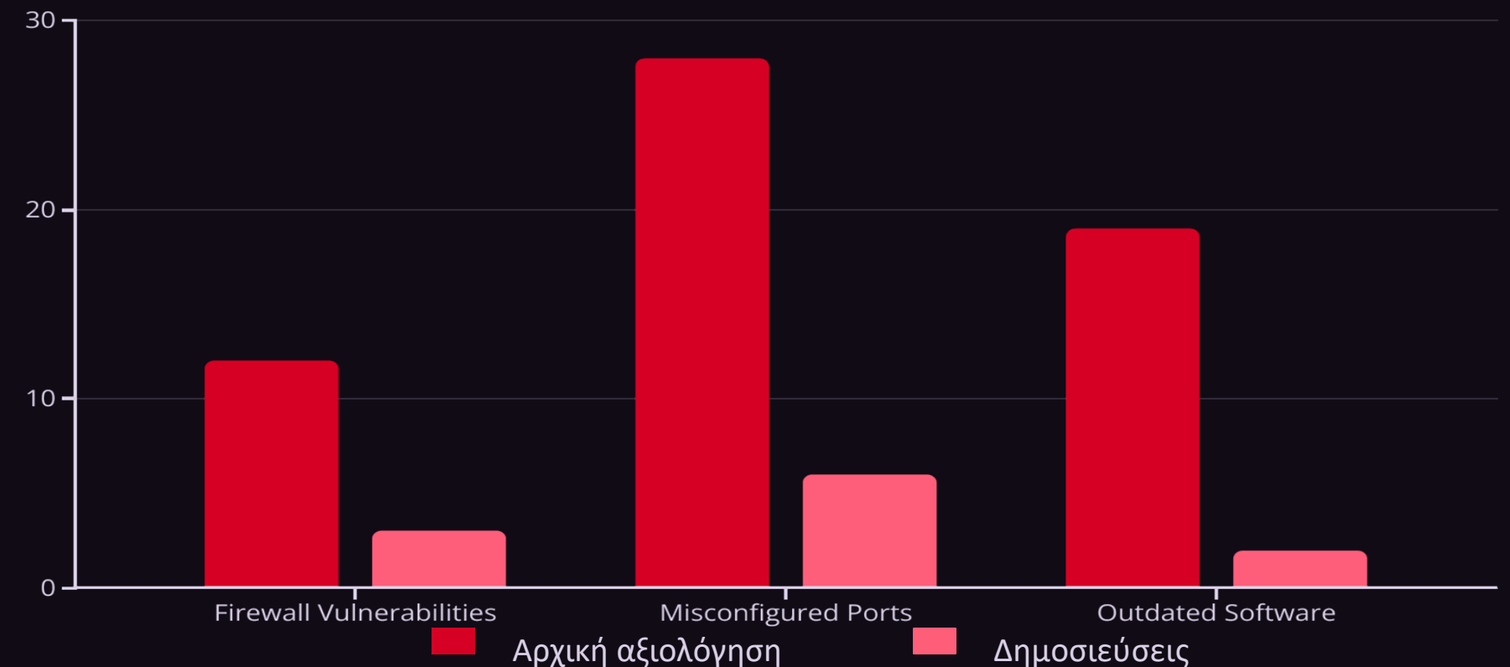
Wireshark

Ένας αναλυτής πρωτοκόλλων δικτύου που ενεργοποιεί δοκιμές διείσδυσης για να καταγράφουν, να επιθεωρούν και να αναλύουν την κίνηση του δικτύου, βοηθώντας στον εντοπισμό ευπαθειών ασφάλειας και στην κατανόηση της συμπεριφοράς του δικτύου.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Δοκιμές διείσδυσης στο δίκτυο

Οι δοκιμές διείσδυσης στο δίκτυο είναι κρίσιμο εξάρτημα των ολοκληρωμένων αξιολογήσεων κυβερνοασφάλειας. Περιλαμβάνει τη συστηματική διερεύνηση και εκμετάλλευση ευπαθειών στην υποδομή δικτύου μιας οργάνωσης για τον εντοπισμό σημείων εισόδου για φορείς.



Το διάγραμμα απεικονίζει τη μείωση των ευπαθειών του δικτύου μετά την υλοποίηση από την οργάνωση των συστάσεων που προέκυψαν από τη δοκιμή διείσδυσης δικτύου. Με τη αντιμετώπιση των αδυναμιών του τείχους (ηλεκτρονικής) προστασίας, των λανθασμένα ρυθμισμένων θυρών και του ξεπερασμένου λογισμικού, η κατάσταση ασφαλείας του δικτύου βελτιώθηκε σημαντικά.

Δοκιμές διείσδυσης σε εφαρμογές ιστού

Οι δοκιμές διείσδυσης των εφαρμογών ιστού είναι ουσιώδεις για την αποκάλυψη ευπαθειών που θα μπορούσαν να εκμεταλλευτούν από κακόβουλους φορείς. Οι δοκιμαστές χρησιμοποιούν προηγμένες τεχνικές για να εντοπίσουν και να εκμεταλλευτούν ευπάθειες στην αρχιτεκτονική των εφαρμογών ιστού, την ταυτοποίηση χρήστη, την εξουσιοδότηση και την επικύρωση εισόδου δεδομένων.

Προσομοιώνοντας πραγματικές επιθέσεις, οι δοκιμαστές διείσδυσης μπορούν να αξιολογήσουν τον πραγματικό κίνδυνο και τον αντίκτυπο των ευπαθειών των εφαρμογών ιστού, ενεργοποιώντας έτσι τις προσπάθειες αποκατάστασης και ενισχύοντας τη συνολική τους κατάσταση ασφαλείας.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Δοκιμές διείσδυσης σε κινητές εφαρμογές

Ευπάθειες εφαρμογών

Εντοπίστε ευπάθειες ασφαλείας στον κώδικα προγραμματισμού για εφαρμογές κινητών, στην αποθήκευση δεδομένων και στα πρωτόκολλα επικοινωνίας που θα μπορούσαν να εκμεταλλευτούν από επιτιθέμενους.

Επαλήθευση χρήστη

Δοκιμές για μηχανισμούς ταυτοποίησης χρηστών που επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα χαρακτηριστικά και δεδομένα εφαρμογής.

Διαρροή δεδομένων

Αποκάλυψη ευαίσθητων πληροφοριών, όπως διαπιστευτήρια και προσωπικά δεδομένα, που θα μπορούσαν να εκτεθούν από την εφαρμογή για κινητά.

Παρακολούθηση θέσης

Αξιολογήστε τις δυνατότητες γεωεντοπισμού της εφαρμογής και εντοπίστε δυνητικούς κινδύνους για την προστασία της ιδιωτικής ζωής ή την κατάχρηση των δεδομένων τοποθεσίας.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Δοκιμές διείσδυσης σε υποδομές νέφους

Οι δοκιμές διείσδυσης της υποδομής του νέφους (cloud) είναι ζωτικής σημασίας για τον εντοπισμό ευπαθειών και την επικύρωση της ασφάλειας των περιουσιακών στοιχείων μιας οργάνωσης που βασίζονται στο νέφος. Οι δοκιμαστές χρησιμοποιούν σειρά τεχνικών για να αξιολογήσουν την ασφάλεια των υπηρεσιών νέφους, των εικονικών μηχανών, των containers και των σχετικών cloud-native τεχνολογιών

Έλεγχος διαρθρώσεων νέφους

Οι δοκιμαστές διείσδυσης εξετάζουν τις διαρθρώσεις των cloud για να εντοπίσουν λανθασμένες ρυθμίσεις, υπερβολικά χαλαρούς ελέγχους πρόσβασης και άλλες αδυναμίες που θα μπορούσαν να εκμεταλλευτούν από επιτιθέμενους.

Δοκιμές ασφάλειας API

Οι δοκιμαστές εξετάζουν την ασφάλεια των APIs που βασίζονται στο cloud, αξιολογώντας την ταυτοποίηση χρήστη, την εξουσιοδότηση χρήστη και την επικύρωση εισόδου δεδομένων για την αποκάλυψη ευπαθειών που θα μπορούσαν να οδηγήσουν σε παραβιάσεις δεδομένων ή παραβιάσεις του συστήματος.

Αξιολογήσεις ασφάλειας εμπορευματοκιβωτίων (container)

Οι δοκιμές διείσδυσης σε περιβάλλοντα με container, συμπεριλαμβανομένων των Docker και Kubernetes, βοηθούν στον εντοπισμό δυνητικών ευπαθειών σε εικόνες container, διαμορφώσεις χρόνου εκτέλεσης και πλαίσια ενορχήστρωσης.

Διαχείριση ταυτότητας και πρόσβασης στο Νέφος

Οι ελεγκτές αξιολογούν την ασφάλεια των συστημάτων διαχείρισης ταυτότητας και πρόσβασης (IAM) που βασίζονται στο νέφος, αξιολογώντας τα προνόμια των χρηστών, τους ελέγχους πρόσβασης βάσει ρόλων και τις οδούς κλιμάκωσης προνομίων.

Επιθέσεις κοινωνικής μηχανικής

- Phishing: Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που έχουν σχεδιαστεί για ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να προβούν σε επιβλαβείς ενέργειες.
- Pretexting: Δημιουργία κατασκευασμένου σεναρίου για τη χειραγώγηση του στόχου ώστε να αποκαλύψει εμπιστευτικά δεδομένα ή να παραχωρήσει μη εξουσιοδοτημένη πρόσβαση.
- Baiting: Αφήνοντας μέσα επικοινωνίας μολυσμένα με κακόβουλο λογισμικό (όπως μονάδες USB) σε δημόσιο χώρο, δελεάζοντας τον στόχο να τα εισάγει στη συσκευή του.

Αντιμετώπιση και αποκατάσταση περιστατικών

1

Προετοιμασία

Προγραμματισμός λογισμικού αντιμετώπισης περιστατικών και εκπαίδευση του προσωπικού.

2

Ανίχνευση και ανάλυση

Προσδιορίστε το περιστατικό, εκτιμήστε τον αντίκτυπο και συγκεντρώστε στοιχεία

3

Περιορισμός και εξάλειψη

Περιορίστε τη ζημιά, αφαιρέστε την απειλή και αποκαταστήστε την κανονική λειτουργία.

4

Ανάκαμψη και μάθηση

Αποκατάσταση δεδομένων, συστημάτων και υπηρεσιών και τεκμηρίωση των ευρημάτων για τη βελτίωση της μελλοντικής απόκρισης.

Η αποτελεσματική αντιμετώπιση και αποκατάσταση περιστατικών είναι ζωτικής σημασίας για την ελαχιστοποίηση των επιπτώσεων των παραβιάσεων ασφαλείας και τη διασφάλιση της ανθεκτικότητας της οργάνωσης. Αυτή η δομημένη προσέγγιση περιλαμβάνει την προετοιμασία για τα περιστατικά, την ταχεία ανίχνευση και ανάλυσή τους, τον περιορισμό της ζημίας και τελικά την ανάκαμψη, μαθαίνοντας παράλληλα από την εμπειρία.

Κανονιστική συμμόρφωση και δοκιμές διείσδυσης

Οι δοκιμές διείσδυσης διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της κανονιστικής συμμόρφωσης. Οι οργανώσεις πρέπει να συμμορφώνονται με ειδικά πρότυπα και κανονισμούς του κλάδου, όπως το PCI-DSS, το HIPAA και το GDPR, τα οποία επιβάλλουν τακτικές αξιολογήσεις ασφαλείας για τον εντοπισμό και τον μετριασμό των ευπαθειών.

Οι δοκιμές διείσδυσης βοηθούν τις οργανώσεις να επιδείξουν συμμόρφωση, παρέχοντας αποδείξεις για τα μέτρα ασφαλείας τους και την αποτελεσματικότητα των στρατηγικών διαχείρισης κινδύνων. Οι λεπτομερείς αναφορές που παράγονται από αυτές τις δοκιμές χρησιμεύουν ως τεκμηρίωση για τους ρυθμιστικούς φορείς και τους ελεγκτές.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Βέλτιστες πρακτικές δοκιμών διείσδυσης

Καθορίστε σαφώς το πεδίο εφαρμογής

Καθορίστε τα όρια, τα περιουσιακά στοιχεία και τους στόχους

Ιεράρχηση ευπαθειών

Επικεντρωθείτε στα πιο κρίσιμα ζητήματα που ενέχουν τον υψηλότερο κίνδυνο για την οργάνωση.

Αξιοποιήστε το Ethical Hacking

Χρησιμοποιήστε τις ίδιες τεχνικές και τα ίδια εργαλεία που

Διατηρήστε επαγγελματισμό

Διεξάγετε την αξιολόγηση με ηθικό και νομικό τρόπο και χωρίς να προκαλέσετε ακούσια βλάβη ή ανατροπή.

Πιστοποιήσεις και προσόντα για δοκιμές διείσδυσης

$50K

Μέσος μισθός

Οι δοκιμαστές διείσδυσης με τις κατάλληλες πιστοποιήσεις μπορούν να διεκδικήσουν υψηλό μισθό στην αγορά εργασίας στον κυβερνοχώρο.

100+

Επιλογές πιστοποίησης

Ένα ευρύ φάσμα πιστοποιήσεων για τους επαγγελματίες του τομέα των δοκιμών διείσδυσης είναι διαθέσιμο.

80%

Προτεραιότητα πρόσληψης

Οι εργοδότες συχνά δίνουν προτεραιότητα σε υποψηφίους με αναγνωρισμένες πιστοποιήσεις και προσόντα δοκιμών διείσδυσης.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Δοκιμές διείσδυσης ως υπηρεσία (PTaaS)

Το PTaaS είναι ένα αναδυόμενο μοντέλο όπου οι οργανισμοί αναθέτουν τις ανάγκες τους σε δοκιμές διείσδυσης σε εξειδικευμένους παρόχους κυβερνοασφάλειας. Η προσέγγιση αυτή προσφέρει πολλά πλεονεκτήματα, όπως πρόσβαση σε ειδικούς ελεγκτές, κλιμακούμενους και συνεχή παρακολούθηση της ασφάλειας.

Το PTaaS απλοποιεί τη διαδικασία δοκιμών διείσδυσης, παρέχοντας στις οργανώσεις ολοκληρωμένες αξιολογήσεις και συστάσεις ασφαλείας προσαρμοσμένες στις μοναδικές απαιτήσεις τους, ενώ παράλληλα ελαχιστοποιεί την επιβάρυνση των εσωτερικών ομάδων πληροφορικής.

Δοκιμές διείσδυσης για μικρές και μεσαίες επιχειρήσεις

Οι μικρές και μεσαίες επιχειρήσεις (ΜΜΕ) συχνά αντιμετωπίζουν μοναδικές προκλήσεις στον τομέα της κυβερνοασφάλειας λόγω περιορισμένων πόρων

και ειδικευμένων. Οι δοκιμές διείσδυσης μπορούν να προσφέρουν σε αυτές τις οργανώσεις οικονομικά αποδοτικό τρόπο εντοπισμού και διεύθυνσης των ευπαθειών, προστατεύοντας τα ευαίσθητα δεδομένα και τα κρίσιμα συστήματά τους.

- **Προσαρμοσμένες αξιολογήσεις:** Οι δοκιμές διείσδυσης για μικρομεσαίες επιχειρήσεις μπορούν να προσαρμοστούν ώστε να επικεντρωθούν στους σχετικούς κινδύνους και τους φορείς επιθέσεων που σχετίζονται με τον κλάδο, το μέγεθος και την υποδομή τους.
- **Πρακτικές συστάσεις:** Τα αποτελέσματα των δοκιμών διείσδυσης παρέχουν στις μικρομεσαίες επιχειρήσεις πρακτικές οδηγίες για την ενίσχυση της κατάστασης ασφαλείας τους, δίνοντας προτεραιότητα αποκατάστασης με τον μεγαλύτερο αντίκτυπο.
- **Συμμόρφωση και κανονισμοί:** Οι δοκιμές διείσδυσης μπορούν να βοηθήσουν τις μικρομεσαίες επιχειρήσεις να αποδείξουν τη συμμόρφωση με τα πρότυπα και τους κανονισμούς του κλάδου, όπως HIPAA, το PCI-DSS και το GDPR.

Δοκιμές διείσδυσης για επιχειρήσεις

Οι δοκιμές διείσδυσης είναι ζωτικής σημασίας για τις μεγάλες επιχειρήσεις με σύνθετες και δυναμικές υποδομές ΤΠ. Οι οργανώσεις αυτές αντιμετωπίζουν αυξημένους κινδύνους κυβερνοασφάλειας και πρέπει να διασφαλίσουν την ασφάλεια των εκτεταμένων δικτύων τους, των κρίσιμων εφαρμογών και των ευαίσθητων δεδομένων τους. Οι ολοκληρωμένες δοκιμές διείσδυσης βοηθούν τους πελάτες επιχειρηματικού επιπέδου να εντοπίζουν τις ευπάθειες, να επικυρώνουν τους ελέγχους ασφαλείας και να ενισχύουν τη συνολική τους στάση ασφαλείας.

Το ραβδόγραμμα επισημαίνει τον αριθμό των ευπαθειών που εντοπίστηκαν και το σχετικό κόστος αποκατάστασης σε διάφορες επιχειρηματικές μονάδες μεγάλης επιχείρησης. Αυτά τα λεπτομερή δεδομένα επιτρέπουν στην οργάνωση να ιεραρχεί και να κατανέμει αποτελεσματικά τους πόρους για τη διευθέτηση των πιο κρίσιμων ζητημάτων ασφάλειας.


CyberSecPro
BY NC SA

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Αναδυόμενες τάσεις στις δοκιμές διείσδυσης

1

Αυτοματισμός και αξιολογήσεις με βάση την Τεχνητή Νοημοσύνη

Η άνοδος των εργαλείων με Τεχνητή Νοημοσύνη που μπορούν να σαρώνουν αυτόνομα για ευπάθειες και να εξαπολύουν επιθέσεις για τον εντοπισμό αδυναμιών σε κλίμακα, μειώνοντας τη χειροκίνητη προσπάθεια που απαιτείται για τις δοκιμές διείσδυσης.

2

Προσομοιωμένες επιθέσεις Ransomware

Οι δοκιμαστές διείσδυσης διεξάγουν ρεαλιστικές προσομοιώσεις Ransomware για να αξιολογήσουν την ικανότητα μιας οργάνωσης να εντοπίζει, να ανταποκρίνεται και να ανακάμπτει από αυτές τις απειλές.

Δοκιμές υποδομών Νέφους

Αυξημένη εστίαση στην ασφάλεια των περιβαλλόντων νέφους μέσω ολοκληρωμένων δοκιμών διείσδυσης εφαρμογών, υποδομών και υπηρεσιών που βασίζονται στο νέφος για την αποκάλυψη λανθασμένων ρυθμίσεων και ευπαθειών.

Το μέλλον των δοκιμών διείσδυσης στην κυβερνοασφάλεια

Οι δοκιμές διείσδυσης θα γίνονται όλο και περισσότερο αυτοματοποιημένες και με βάση την Τεχνητή Νοημοσύνη, αξιοποιώντας τη μηχανική μάθηση και τις προηγμένες αναλύσεις για τον εντοπισμό και την εκμετάλλευση ευπαθειών με πρωτοφανή ταχύτητα και κλίμακα. Οι αναδυόμενες τεχνολογίες, όπως η κβαντική υπολογιστική και τα αυτόνομα μη επανδρωμένα αεροσκάφη, θα φέρουν επανάσταση στον τρόπο με τον οποίο οι οργανώσεις αξιολογούν και αμύνονται έναντι των εξελισσόμενων κυβερνοεπιθέσεων.

Η συνεχής παρακολούθηση σε πραγματικό χρόνο και η προδραστική ανίχνευση απειλών θα είναι ο κανόνας, με τις δοκιμές διείσδυσης να ολοκληρώνονται αδιάλειπτα στον κύκλο ζωής της ασφάλειας μιας οργάνωσης. Οι ηθικοί χάκερ θα εργάζονται παράλληλα με έξυπνα συστήματα για να αποκρυπτογραφήσουν κρυμμένους κινδύνους και να επικυρώνουν την αποτελεσματικότητα των ελέγχων ασφαλείας σε σύνθετα, δυναμικά περιβάλλοντα ΤΠ.

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Συμπέρασμα και βασικά στοιχεία

2

1

Η ασφάλεια κυβερνοχώρο παραμένει ύψιστη προτεραιότητ

Οι δοκιμές διείσδυσης αποτελούν κρίσιμο εξάρτημα μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας, βοηθώντας τις οργανώσεις να παραμείνουν εμπρός από τις εξελιγμένες απειλές και να διασφαλίσουν την προστασία των πολύτιμων περιουσιακών τους στοιχείων.

Συμμόρφωση και Διακυβέρνηση

3

Οι τακτικές διείσδυσης βοηθούν τις οργανώσεις να αποδείξουν την κανονιστική τη συμμόρφωση, τον μετριασμό και τη συντήρηση

την εμπιστοσύνη των πελατών και των ενδιαφερομένων μερών.

Η ηθική παραβίαση είναι ουσιώδης

με την εφαρμογή των ίδιων τακτικών και τεχνικών με τους επιτιθέμενους του πραγματικού κόσμου, οι δοκιμές διείσδυσης ενεργοποιούν τις οργανώσεις να αποκαλύπτουν ευπάθειες και να ενισχύουν τις άμυνες ασφαλείας τους.

Συνεχής βελτίωση

Οι συνεχείς δοκιμές διείσδυσης και οι προσπάθειες αποκατάστασης είναι ζωτικής σημασίας για να συμβαδίζουν με το εξελισσόμενο τοπίο της κυβερνοασφάλειας και να διασφαλίζουν τη μακροπρόθεσμη ανθεκτικότητα μιας οργάν

Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Βιβλιογραφικές αναφορές

1. IEEE. (2016). IEEE code of ethics. https://www.ieee.org/about/corporate/governance/p7-8.html
2. ACM Code of Ethics and Professional Conduct (2018). Association for Computing Machinery. https://www.acm.org/code-of- ethics
3. Barquin, R. C. (1992, 7 Μαΐου). In Pursuit of 'Ten Commandments' for Computer Ethics. Computer Ethics Institute. https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics
4. The Ten Commandments of Computer Ethics, Created in 1992 by the Computer Ethics Institute, offer a Foundational Set of principles for ethical computer use (Barquin 1992).
5. European Union Agency for Cybersecurity. (2022). ECSF, European cybersecurity skills framework. Publications office. https://doi.org/10.2824/859537
6. R. Schoon και Kleinaltepohl, Cybersecurity in the Electricity Sector: managing Critical Infrastructure (SpringerLink, 2018).
7. J. R. Vacca, Industrial Cybersecurity for Engineers (Elsevier, 2015).
8. ECSO, "Energy Networks and Smart Grids", Cyber Security for the Energy Sector, WG3, Sectoral Demand, Νοέμβριος 2018 URL: https://.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf
9. ENISA, "Smart Grid Threat Landscape and Good Practice Guide", Δεκέμβριος 2013 URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
10. Άλλες αναφορές που αναφέρονται σε κάθε θέμα της ενότητας ΚΠΣ (CSP module)

Διαφάνεια: Πηγές

1. Περιεχόμενο για βίντεο teaser: Το περιεχόμενο αυτού του βίντεο βασίζεται στο πακέτο λογισμικού 3 Deliverables του CyberSecPro με πολύτιμες συνεισφορές από τους εταίρους των CyberSecPro.
2. Γλωσσική εξειδίκευση: Το παραδοτέο D3.1 πέρασε αυστηρό γλωσσικό έλεγχο λαθών. Αυτό περιελάμβανε τη χρήση της Τεχνητής Νοημοσύνης Grammarly και τη σχολαστική αναθεώρηση από φυσικό ομιλητή της αγγλικής γλώσσας.
3. Περιεχόμενο πολυμέσων: Pictory, Getty images και άλλες βάσεις δεδομένων πολυμέσων.
4. Συνεργασία εταίρων: Αναγνωρίζουμε την προσφορά του CyberSecPro, καθώς και των φωτογραφιών των εκπαιδευτών.
5. Εκπαιδευτικό υλικό: Το εκπαιδευτικό υλικό για αυτή την ενότητα του CyberSecPro παραδόθηκε από εκπαιδευτή που είναι καταχωρημένος στο κατάλογο και τα εύσημα αποδίδονται στους συγγραφείς.
6. Δημιουργική πίστωση: teaser δημιουργήθηκε των πόρων από τον Ευρωπαίο επαγγελματία στον τομέα της κυβερνοασφάλειας Paresh Rathod.
7. Υλικό της κατάρτισης που δημιουργήθηκε με τη χρήση ακαδημαϊκής, ερευνητικής βιβλιογραφίας και Ανοικτού Εκπαιδευτικού Υλικού (OEM) με τις δέουσες αναφορές στους συγγραφείς.
8. Ορισμένο από το υλικό χρησιμοποίησε εργαλεία βασισμένα στην Τεχνητή Νοημοσύνη, συμπεριλαμβανομένων προσομοιωτών φωνής (με τις δέουσες πιστώσεις στους συγγραφείς) για να προσφέρει τις καλύτερες εμπειρίες μάθησης στους συμμετέχοντες.

Εκπαιδευτές: Paresh & Δημήτρης Κούτρας

Συνδεθείτε με το CyberSecPro: Πώς να εγγραφείτε και πρακτικές πληροφορίες

1. Ιστοσελίδα: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn (επαγγελματικό κοινωνικό δίκτυο): https://www.linkedin.com/company/cybers ecpro-euproject/

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

CSP010_W_H:
Εκπαιδευτής: Paresh Rathod, Laurea UAS, Φινλανδία

Σας ευχαριστώ

Παρακαλείστε να στέλνετε όλες τις ερωτήσεις στους εκπαιδευτές (ή/και):
paresh.rathod@laurea.fi

CyberSecPro