

# MILSHIELD SECURITY P.C.



## INFORMATION SECURITY SERVICES DESCRIPTION

“Some organizations will be a target regardless of what they do, but most become a target because of what they do.”



INFORMATION SECURITY SERVICES

## NETWORK PENETRATION TEST

Στις μέρες μας, η επικοινωνία μεταξύ των ανθρώπων αλλά και των εταιρειών είναι σύνηθες να περνάει μέσα από τον κόσμο του Internet. Εγκληματικές οργανώσεις χρησιμοποιούν αυτή την συνήθεια για να αντλήσουν χρήσιμες για αυτούς πληροφορίες μέσα από διάφορες αδυναμίες στην ασφάλεια του διαδικτύου. Στην Milshield αναλαμβάνουμε να κάνουμε το internet και τις επικοινωνίες σας μέσα από αυτό πιο ασφαλείς.

Οι επιτιθέμενοι μπορούν να βρίσκονται οπουδήποτε στο πλανήτη και το μόνο που χρειάζονται είναι πρόσβαση στο διαδύκτιο. Η απειλή είναι **πραγματική** και συμβαίνει **καθημερινά**.

Η MILSHIELD πάντα με την σύμφωνη γνώμη του ιδιοκτήτη του δικτύου μπορεί να πράξει ως ένας πραγματικός επιτιθέμενος (hacker) και να προσομειώσει τον κακόβουλο εισβολέα.

Εκτελούμε σενάρια επίθεσης αξιοποιώντας όλα τα συγχρόνα μέσα και μεθόδους διείσδυσης στο δίκτυο και τις υποδομές σας μέχρις ως ότου πέσει η άμυνα του πληροφοριακού σας συστήματος. Στόχος μας είναι η ανακαλύψη και κατά συνέπεια η εξασφάλισή σας από τυχόν κενά ασφαλείας (breaches) που θα προκύψουν.

## METHODOLOGY WHO?

### 1. Footprinting / Network Mapping

Η διαδικασία του footprinting είναι μια καθόλα νόμιμη διαδικασία που έχει ως σκοπό να συλλέξει όσο των δυνατόν περισσότερες πληροφορίες σχετικά με τον "στόχο" και των συστημάτων που χρησιμοποιεί.

Η διαδικασία αυτή εμπλέκει τόσο τεχνικά όσο και μη τεχνικά μέσα, μπορεί να περιέχει αναζήτηση σε διάφορες "βιβλιο θήκες" στο internet για πληροφορίες σχετικά με τον στόχο (whois databases, domain registers, mailing lists κλπ).

Οι συμβουλοί ηλεκτρονικής ασφαλείας της MILSHIELD συλλεγουν κατά το δυνατό επιπλέον πληροφορίες απαραίτητες για την δημιουργεία ενός topology and network profile.

Τέτοιες πληροφορίες αφορούν διευθύνσεις IP, συλλογή εταιρικών πληροφοριών από public domains, Ping sweeps, port scanning κτλ.

Οι πληροφορίες αυτές μετά την συλλογή τους κατηγοριοποιούνται και αναλύονται να μενόμενα αποτελέσματα:

- Domain Names
- Server names
- Ip addresses
- Network Topology
- Company profile

Ενέργειες για επίτευξη Αναμενόμενων Αποτελεσμάτων:

- Καθορισμός εύρους IP
- Ανάλυση DNS Servers
- Αναγνώρηση των συστημάτων που χρησιμοποιούνται καθώς και των συσκευών μεταξύ τους
- Αναγνώρηση εταιρικών e-mail
- Έυρεση διαφόρων πηγών πληροφοριών για την εταιρεία (Forums, news groups κλπ)
- Ανάλυση της εταιρικής ιστοσελίδας

# MILSHIELD

## INFORMATION SECURITY SERVICES

### NETWORK PENETRATION TEST

#### 2. Scanning and Enumeration

Στόχος αυτής της διαδικασίας είναι η πιο τεχνική και σε βάθος ανάλυση των συστημάτων όπως πχ ανοιχτές πόρτες και services που τρέχουν σε αυτές, κανόνες των firewall κ.α. και περιλαμβάνει μία πιο ενεργή και αναλυτική προσέγγιση στην ανίχνευση των στοχοποιημένων συστημάτων.

Αναμενόμενα αποτελέσματα:

- Ανάλυση όλων των πορτών [ανοιχτές, κλειστές, φιλτραρισμένες]
- IP Addresses από τα συστήματα
- IP Addresses από τοπικά δίκτυα
- Ανάλυση του δικτύου
- Αναγνώριση πρωτοκόλλων που χρησιμοποιούνται
- Αναγνώριση πρωτοκόλλων routing
- Τύπος των Operating Systems που χρησιμοποιούνται
- Τύπος των Application και το Patch Level αυτών

Ενέργειες για επίτευξη Αναμενόμενων Αποτελεσμάτων:

- Συλλογή των responses από το δίκτυο
- Δοκιμή TTL / firewalking firewall
- Χρήση ICMP για την ανεύρεση των συσκευών στο δίκτυο
- Χρήση TCP και UDP σε διάφορες πόρτες [20, 21, 80, 443] σε hosts του δικτύου
- Αναγνώριση Standard protocols
- Αναγνώριση non-Standard protocols
- Αναγνώριση encrypted protocols
- Προσδιορισμός ώρας-ημερομηνίας που χρησιμοποιείται και System Up-Time
- Ανάλυση των DNS Servers

#### 3. Vulnerability Analysis

Επειτα από την ολοκλήρωση των προηγούμενων φάσεων και την συλλογή των πληροφοριών ο penetration tester θα προσπαθήσει να ανακαλύψει όλες τις ευπάθειες των συστημάτων που χρησιμοποιούνται και να τις καταγράψει.

Για τον σκοπό αυτό χρησιμοποιούνται διάφορα αυτοματοποιημένα εργαλεία που δοκιμάζουν τα συστήματα για όλες τις μέχρι εκείνη την στιγμή γνωστές ευπάθειες.

Πέρα από αυτό ο penetration tester θα κάνει και δοκιμές [manually] για τυχόν ευρήματα που δεν είναι καταγεγραμμένα.

Αναμενόμενα αποτελέσματα:

- Καταγραφή τύπου των Applications και services ανά ευπάθεια
- Patch level των συστημάτων και application
- Καταγραφή των ευπαθειών που μπορεί να χρησιμοποιηθούν για DOS επιθέσεις

Ενέργειες για επίτευξη Αναμενόμενων Αποτελεσμάτων:

- Ενσωμάτωση των scanners, hacking tools και exploits
- Καταγραφή των ευπαθειών
- Δοκιμή των ευπαθειών που εντοπίστηκαν χρησιμοποιώντας exploits

# MILSHIELD

INFORMATION SECURITY SERVICES

## NETWORK PENETRATION TEST

### 4. Exploitation

Κατά την διάρκεια αυτής της φάσης δοκιμάζονται διάφορα exploits σε ευπάθειες που έχουν εντοπιστεί.

Παραδείγματα τέτοιων δοκιμών είναι:

- Buffer overflows
- Application or system configuration problems
- Modems
- Routing issues
- DNS attacks
- Address spoofing
- Share access and exploitation of inherent system trust relationships.

### 5. Reporting

Το τελικό στάδιο είναι αυτό του reporting. Σε αυτό καταγράφονται όλα τα ευρήματα του test και περιέχει τόσο τεχνικά όσο και μη τεχνικά θέματα.

Αναλύονται οι ευπάθειες που έχουν εντοπιστεί και καταγραφεί και μέσα από διάφορες απεικονίσεις (screenshots, διαγράμματα) δίνεται πλήρη αναφορά για αυτά.

# MILSHIELD

INFORMATION SECURITY SERVICES

## WEB APPLICATION PENETRATION TEST

Οι Web Based εφαρμογές (sites, portals, API) έχουν γίνει εξαιρετικά ευπαθείς σε διάφορες μορφές επίθεσης από hacker. Σύμφωνα με report(Gartner) το 75% των επιθέσεων σήμερα πραγματοποιούνται σε αυτό το επίπεδο (application level)

Παρά την χρήση διαφόρων συσκευών αμύνης όπως Firewalls, IDS, IPS κ.α. οι hackers είναι δυνατό να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα, να κλείσουν websites και servers και να εξαπατήσουν επιχειρήσεις και οργανισμούς χωρίς την δυνατότητα να αντιμετωπιστούν και ορισμένες φορές ακόμη και να ανακαλυφθούν.

Για να αντιμετωπίσουμε αυτό το πρόβλημα προσφέρουμε μια ολοκληρωμένη λύση μέσα από ένα Web Application Penetration Test. Μέσα από αυτό το test μπορούμε να εντοπίσουμε αναλύσουμε και καταγράψουμε τις ευπάθειες που παρουσιάζονται σε ένα Web Application και στην συνέχεια να τις αντιμετωπίσουμε ασφαλίζοντας έτσι την εφαρμογή.

## METHODOLOGY WHO?

### 1. Configuration Management Analysis

Αξιολογείται η υποδομή που χρησιμοποιεί η εφαρμογή από τους αναλυτές της MILSHIELD.

Οι δοκιμές που θα γίνουν είναι οι κάτωθι:

- TLS και SSL δοκιμές
- Δοκιμές στην βάση δεδομένων που χρησιμοποιεί το σύστημα διαχείρησης
- Δοκιμές στις υποδομές (hardware) και την σχέση του με την εφαρμογή, ανάλυση των ευπαθειών που πιθανών παρουσιάζονται, ανάλυση του μηχανισμού αυθεντικοποίησης και αναγνώριση των θυρών που χρησιμοποιεί η εφαρμογή.
- Ανάλυση των ρυθμίσεων που έχουν γίνει, αναζήτηση σε αρχεία και φακέλους, ανάλυση τυχόν σχολιών από web developers και και ανάλυση των logs της εφαρμογής.
- Αναζήτηση και ανάλυση για παλιά αρχεία, backups, logs και διάφορα αρχεία που χρησιμοποιεί η εφαρμογή.
- Δοκιμή μεθόδων HTTP που υποστηρίζονται και η πιθανότητα για XST (Cross - Site Tracing)

### 2. Scanning and Enumeration

Αξιολογούνται οι μηχανισμοί που χρησιμοποιεί η εφαρμογή για την αυθεντικοποίηση.

Οι δοκιμές που θα γίνουν είναι οι κάτωθι:

- Διαχείριση των credentials
- Καταγραφή των λογαριασμών χρηστών που είναι εύκολα αναγνωρισμοί (πχ admin, user κ.α.)
- Διενέργεια δοκιμών στους μηχανισμους αυθεντικοποίησης.
- Ανάλυση του μηχανισμού αποσύνδεσης και τις αδυναμίες που σχετίζονται με την μνήμη cache του browser.
- Δοκιμές αντοχής σε μηχανισμούς CAPTCHA και δοκιμές σε πολλαπλούς μηχανισμούς αυθεντικοποίησης

# MILSHIELD

INFORMATION SECURITY SERVICES

## WEB APPLICATION PENETRATION TEST

### 3. Session management analysis

Αξιολόγηση των διαφόρων μηχανισμών διαχείρισης του session της εφαρμογής.

- Δοκιμή του μηχανισμού διαχείρισης των sessions
- CSRF (Cross-Site Request forgery)
- Ανάλυση των χαρακτηριστικών των Cookies

### 4. Analysis of Authorization

Αξιολόγηση των μηχανισμών αδειοδότησης.

- Κλιμάκωση των δικαιωμάτων
- “path traversal”
- Ανάλυση της λογικής της εφαρμογής και καταγραφή τυχόν λαθών που μπορεί να χρησιμεύσουν στην αλλοίωση δικαιωμάτων

### 5. Data Validation Analysis

- Δοκιμές XSS
- Δοκιμές SQL Injection
- Δοκιμές LDAP injection
- Δοκιμές XML injection
- Δοκιμές SSI injection
- Δοκιμές XPath injection
- Δοκιμές IMAP/SMTP injection
- Code injection
- Δοκιμή για injection σε Operating system commands
- Ανάλυση για buffer overflow
- Δοκιμή για Splitting/Smuggling στο πρωτόκολλο HTTP

### 6. Analysis of Web Services

- Δοκιμές ασφαλείας στη WSDL
- Δοκιμές ασφαλείας στο περιεχόμενο του παραγόμενου XML
- Δοκιμή των παραμέτρων REST - HTTP GET
- Δοκιμή για ευπάθειες AJAX

### 7. Reporting

Η τελική φάση της διαδικασίας είναι η σύνταξη του report που περιέχει ανάλυση των ενεργειών που έχουν γίνει, ευπάθειες που έχουν εντοπισθεί και προτάσεις για την αντιμετώπηση τους

Το τελικό Report θα είναι διαθέσιμο και κατάλληλα προετοιμασμένο για ανάγνωση και ανάλυση και από το τεχνικό τμήμα και το τμήμα διαχείρησης.

# MILSHIELD

## INFORMATION SECURITY SERVICES

### PENETRATION TEST

Κάθε Penetration Test μπορεί να περιέχει τα κάτωθι modules για να ταιριάξει στις ανάγκες σας:

#### 1. Internet Security Assessment

Οποιαδήποτε συσκευή είναι συνδεδεμένη στο Internet είναι και πιθανός στόχος ενός Hacker. Στην Milshield παρέχουμε ανάλυση των ευπαθειών κατά την οποία καταγράφουμε την αρχιτεκτονική του δικτύου, ανοιχτές πόρτες στο διαδίκτυο, hosts και services συνδεδεμένα σε αυτό και διασφαλίζουμε ότι αυτές οι διαδικτυακές συσκευές είναι ασφαλείς.

Συγκεντρώνουμε πληροφορίες όπως domain names, εύρος IP, λειτουργικά συστήματα και εφαρμογές για να εντοπίσουμε συστήματα με πρόσβαση στο διαδίκτυο, πως αυτά συνδέονται μεταξύ τους και services τα οποία εκτίθενται σε αυτό (HTTP, SMTP, terminal services).

Όταν ολοκληρωθεί η φάση αυτή ελέγχουμε αν το κάθε service που τρέχει στις συσκευές είναι ενημερωμένο και καταγράφουμε διάφορες ευπάθειες που μπορεί να αντιμετωπίσουν.

Έπειτα προχωρούμε στην προσπάθεια διείσδυσης στο δίκτυο (Penetration Test) όπου χρησιμοποιούμε τις πληροφορίες που έχουμε συλλέξει και δρούμε όπως ο επιτιθέμενος(hacker).

Μετά από όλες αυτές τις ενέργειες συντάσσουμε το report που περιέχει αναλύση των ευπαθειών που εντοπίστηκαν και προτάσεις για την ενίσχυση της ασφάλειας του δικτύου.

#### 2. Intranet Security Assessment

Όπως και με τις εξωτερικές απειλές μέσω διαδικτύου, οι επιχειρήσεις θα πρέπει να προστατευτούν και από εσωτερικές απειλές μέσω του τοπικού τους δικτύου.

Εδώ χρησιμοποιούμε παραπλήσιες τακτικές και μεθόδους με το Internet Security Assessment και παρέχουμε ανάλυση και αξιολόγηση κινδύνου για την προστασία από ενδεχόμενες απειλές από εσωτερικούς κακόβουλους χρήστες.

#### 3. Web Application Assessment

Η αξιολόγηση αυτή εξετάζει τις πληροφορίες και υπηρεσίες που προσφέρονται μέσα από Web Based εφαρμογές (Portals, E-commerce) και έχει ως στόχο την διασφάλιση της εμπιστευτικότητας, ακεραιότητας, την πιστοποίηση και ακεραιότητα των προσωπικών δεδομένων των καταναλωτών.

Επίσης προσφέρουμε ανάλυση του πηγαίου κωδικά των εφαρμογών για την αποτελεσματικότερη διασφάλιση των εφαρμογών στο περιβάλλον.

#### 4. Wireless Assessment

Τα ασύρματα δίκτυα αν και προσφέρουν ευελιξία στην χρήση και δεν περιορίζονται στα φυσικά όρια ενός παραδοσιακού τοπικού δικτύου είναι πιο ευάλωτα σε ευπάθειες και απειλές.. Με το Wireless Assessment γίνεται αξιολόγηση αυτών των τεχνολογιών με στόχο την αποτροπή τυχόν υποκλοπών και μη εξουσιοδοτημένων προσβάσεων.

Παρέχουμε ανάλυση των κρυπτογραφημένων δικτύων που μπορεί να είναι ευάλωτα και διασφαλίζουμε την ασφάλεια του δικτύου.

# MILSHIELD

## INFORMATION SECURITY SERVICES

### PENETRATION TEST

#### 5. Forensic Analysis

Εκτός από την πρόληψη μελλοντικών επιθέσεων, μπορούμε να διεξάγουμε εγκληματολογική ανάλυση για την αξιολόγηση προηγούμενων παραβιάσεων ασφάλειας.

Η ανάλυση αυτή εξετάζει log reports, συγκρίνει αντίγραφα ασφαλείας για τον εντοπισμό τροποποιήσεων στο δίκτυο, και ερευνά την εισαγωγή ξένων εργαλείων λογισμικού για να βοηθήσει στον εντοπισμό εισβολέων. Καθορίζει το βαθμό στον οποίο το δίκτυο έχει παραβιαστεί, και την άμβλυνση πιθανών ζημιών από την εισβολή.

#### 6. Physical Security Assessment

Η πρόσβαση σε εμπιστευτικές πληροφορίες μπορεί συχνά να επιτευχθεί με απλή αποκτήσουν φυσική πρόσβαση στους χώρους της εταιρείας.

Διεξάγουμε επί τόπου ελέγχους για την αξιολόγηση της φυσικής ασφάλειας και χρησιμοποιούμε τεχνικές που έχουν σχεδιαστεί για να αποκτήσουν φυσική πρόσβαση σε ασφαλείς περιοχές και στο σύστημα του δικτύου.

#### 7. Database Assessment

Λίστες πελατών, στοιχεία πιστωτικών καρτών, καθώς και άλλες εμπιστευτικές πληροφορίες που περιέχονται σε βάσεις δεδομένων θα πρέπει να τύχουν ιδιαίτερης προστασίας από μη εξουσιοδοτημένη πρόσβαση.

Δοκιμάζουμε την ακεραιότητα της βάσης δεδομένων για να διαπιστωθεί αν κάποια ευπάθεια μπορεί να θέσει σε κίνδυνο αυτές τις ευαίσθητες πληροφορίες.

#### 8. Intrusion Investigation

Μπορούμε να διερευνήσουμε τεκμηριωμένες απόπειρες εισβολής μέσα στο δίκτυο σας και περιπτώσεις όπου τα δεδομένα ήταν πραγματικά σε κίνδυνο. Μέσω της έρευνας, μπορείτε να βρείτε την πηγή της επίθεσης, οι τεχνικές που χρησιμοποιήθηκαν, και πώς μπορείτε να διορθώσετε τις ατέλειες αυτές.

Ενώ είναι πάντα καλύτερο κανείς να σταματήσει τις επιθέσεις προτού να συμβουν, είναι επίσης σημαντικό να διερευνήθει και κάθε πιθανή παραβίαση της πνευματικής σας ιδιοκτησίας.



## MILSHIELD P.C.

Telephone : 210 983 5124  
Fax : 210 800 8299  
E-mail : [info@milshield.gr](mailto:info@milshield.gr)  
[www.milshield.gr](http://www.milshield.gr)

Postal Adress:  
MilShield P.C  
118 Amfitheas Av.  
P.Faliro, P.C 17562.