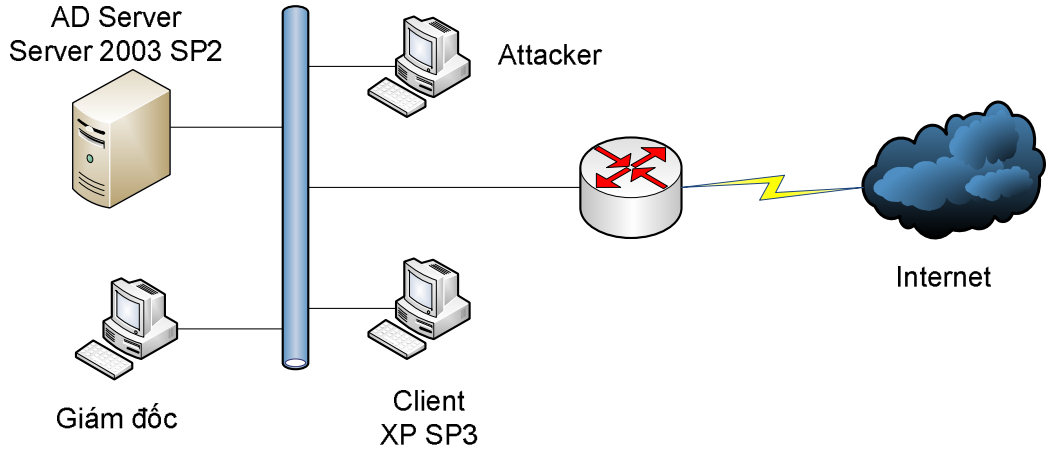
ĐỀ THI THỰC HÀNH 2011
TẠI CUỘC THI "SINH VIÊN VỚI ATTT"

A. ĐỀ THI THỨ NHẤT:

Thời gian làm bài : 30 phút

Ta có sơ đồ mạng sau



Mô tả sơ đồ mạng:

- Cấu hình Window Server 2003 làm các chức năng sau cho
  - DHCP Server
  - DNS Server
  - Acitve Directory Server
  - IIS Server version 6.0 (web server)
- Các client trong mạng điều là thành viên bên trong domain.
- Một máy client sử dụng window xp sp3 . Trên máy XP SP 3 có các user : client 1, client 2, client 3, và user admin , có quyền quản lý toàn bộ hệ thống. Trong 3 user client trên, có 2 user đặt password ít hơn 7 ký tự (4 ký tự) và 1 client đặt passowrd nhiều hơn 7 ký tự
- Giả sử bạn là 1 user thường (attacker) chung một mạng LAN như sơ đồ trên.

Yêu cầu :

Phần 1 : Phát hiện lỗ hổng trong mạng

Tổng số điểm : 30

Câu 1: Sinh viên thực hiện

1.1 Cài đặt chương trình scan để xác định IP của máy Client SP3, Server 2003, Giám đốc (2 điểm)

1.2 Cài đặt Nmap trên máy đóng vai trò attacker (1 điểm)

1.3 Cài đặt Nessus trên máy đóng vai trò attacker (1 điểm)

1.4 Cài đặt metasploit trên máy attacker (1 điểm)

Câu 2 : Xác định các dịch vụ

2.1 Xác định phiên bản hệ điều hành các máy trong mạng.(1điểm)

2.2 Xác định các port đang mở trên máy tính. (1điểm)

2.3 Xác định các dịch vụ tương ứng với các port (2điểm)

Câu 3 : Sử dụng Nmap và Nessus để scan các vulnerability (lổ hổng) trên máy client xp sp3.

3.1 Sử dụng Script Engine của Nmap để scan lỗi hệ điều hành (1 điểm)

3.2 Sử dụng Nessus để scan lỗi (1điểm)

3.3 Xác định lỗi cho phép từ xa truy cập và thực thi trái phép vào máy XP SP3 (5 điểm)

Câu 4 : Khai thác lổ hổng

4.1 Sử dụng chương trình Cain Abel hoặc Ettercap để thực hiện thu thập file SAM chứa username và hash của password trên máy XP SP3 (1 điểm)

4.2 Dựa trên file SAM xác định 2 user có chiều dài password nhỏ hơn 7 (4 ký tự) ký tự trên máy XP SP 3 (2 điểm).

4.3 Thực hiện quá trình crack password bằng công cụ Cain Abel hoặc Ophcrack, … của 2 user client trên. (2 điểm)

4.4 Xác định các lỗi MS10-065 và dùng Denial of Service IIS Server. (3 điểm)

4.5 Kiểm tra lỗi WebDav Auth By Pass exploit trên IIS 6.0 (3 điểm)

4.6 Thực thi quá trình attacker có thể dựa vào máy XP SP3 để chiếm quyền điều khiển máy Server (3 điểm)

Phần 2 : Đưa ra hướng khắc phục lổ hổng

Tổng số điểm : 30

Câu 1: Sinh viên đưa ra giải pháp khắc phục lỗi cho phép truy cập và thực thi từ xa máy XP SP 3 (20 điểm)

Câu 2 : Sinh viên đưa ra giải pháp khắc phục lỗi WebDav by Pass Exploit trên Server (10 điểm)

Lưu ý :

Sinh viên có thể sử dụng các công cụ Nmap, Wireshark, GFI , Metasploit, Firefox, Ophcrack, Hasmter…

Sinh viên nên tìm kiếm thông tin các lỗi trên trang Microsoft, Inj3ct0r.com, exploit-db.com.

B. ĐỀ THI THỨ HAI

1. Mô tả hệ thống:

Cho một hệ thống mạng cùng chung 1 dải IP trong LAN bao gồm:

- Một File Server
- Một Server có Web Server và FTP Server
- Ba máy PC client dành cho thí sinh

Một số thông tin về hệ thống:

- Về hệ thống mạng thí sinh chỉ biết được địa chỉ IP của 3 máy Client dành cho thí sinh.
- Thí sinh biết thông tin về username và password quản trị của File Server (user: administrator ; pass: a@123456). Tuy nhiên hiện tại thí sinh chưa biết được địa chỉ IP của File Server.
- Trên các máy client có cài đặt sẵn chương trình Wireshark và thư mục chức các shell code cho thí sinh lựa chọn để sử dụng khi cần thiết.

2. Yêu cầu của đề thi:

Phần 1: Xác định thông tin hệ thống

- Hãy xác định địa chỉ IP chính xác của 2 Server trên hệ thống mạng đã cho.(IP của 3 máy này nằm trong dải 192.168.0.1 – 192.168.0.15). Thí sinh chỉ sử dụng các công cụ có sẵn trên các máy. - *Mỗi địa chỉ IP chính xác thí sinh được …… điểm.*

Phần 2: Quản trị, cấu hình phân quyền cho File Server

Trong công ty có ketoan1,ketoan2 là của phòng kế toán;Kinhdoanh1,kinhdoanh2 là của phòng KinhDoanh. Và File Server dùng để chứa dữ liệu của phòng kế toán và kinh doanh. Trên File Server có folder : Ketoan – chứa dữ liệu của phòng Kế Toán,folder : KinhDoanh – chứa dữ liệu của phòng KinhDoanh.

- Yêu cầu cho thí sinh

1. Cấu hình chỉ cho Ketoan1,ketoan2 truy cập vào được folder Ketoan nhưng không truy cập được folder KinhDoanh. Thực hiện được ý này đội thi sẽ nhân được……điểm.

2. Cấu hình cho kinhdoanh1,kinhdoanh2 truy cập vào folder KinhDoanh nhưng không truy cập được folder Ketoan.Thực hiện được ý này đội thi sẽ nhân được……điểm.

3. Cấu hình trên File Server sao cho user Ketoan1 được đọc, sửa ,xóa, tạo mới file trên thư mục Ketoan. User : ketoan2 chỉ được đọc file trên thư mục Ketoan, không được sửa, xóa. Thực hiện được ý này đội thi sẽ nhân được……điểm.

4. Cấuhình trên File Server saocho user kinhdoanh2 chỉđượcđọc,ghi file trênthưmụcKinhdoanh, khôngđượcsửa, xóa,thực thi. Thựchiệnđược ý nàyđộithisẽnhânđược……điểm

Phần 3: Phân tích traffic mạng tìm thông tin

1. Sử dụng wireshark để phân tích gói dữ liệu **forensics1.cap** đã thu thập được trên mạng để tìm ra:
   - Từ dữ liệu thu thập được xác định xem các máy đang thực hiện tác vụ gì ? *Thực hiện được ý này đội thi sẽ nhân được……điểm.*
   - Xác định Username và Password chính xác của người sử dụng dịch vụ. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

2. Sử dụng wireshark để phân tích gói dữ liệu **forensics2.cap,** đây là dữ liệu trao đổi SMTP thu thập được trên mạng, hãy xác định:

- Xác định chính xác 2 địa chỉ email của người nhận và người gửi email. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*
- Xác định nội dung của email trao đổi.*Thực hiện được ý này đội thi sẽ nhân được……điểm.*

3. Sử dụng wireshark để phân tích gói dữ liệu **forensics3.cap,** đây là dữ liệu xác thực SMTP thu thập được trên mạng, hãy xác định:
   - Xác định chính xác username và password của người sử dụng xác thực. (gợi ý username và password sử dụng mã hóa). *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

4. Sử dụng wireshark để phân tích gói dữ liệu **forensics4.cap,** đây là dữ liệu HTTP authentication thu thập được, hãy xác định:
   - Xác định chính xác username và password của người sử dụng xác thực. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

Phần 4: Xâm nhập máy chủ

Thí sinh tìm cách xâm nhập vào máy chủ có FTP Server và WebServer để thực hiện một số yêu cầu sau:<chú ý tài khoản FTP là tài khoản đã xác định được ở **phần 3>**

1. Upload được file có dạng Tendoi.txt vào thư mục **www** của máy chủ web.(*Test http://192.168.0.x/tendoi.txt .). Thực hiện được ý này đội thi sẽ nhân được……điểm.*

2. Xác định chính xác tên của các tài khoản trên Server. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

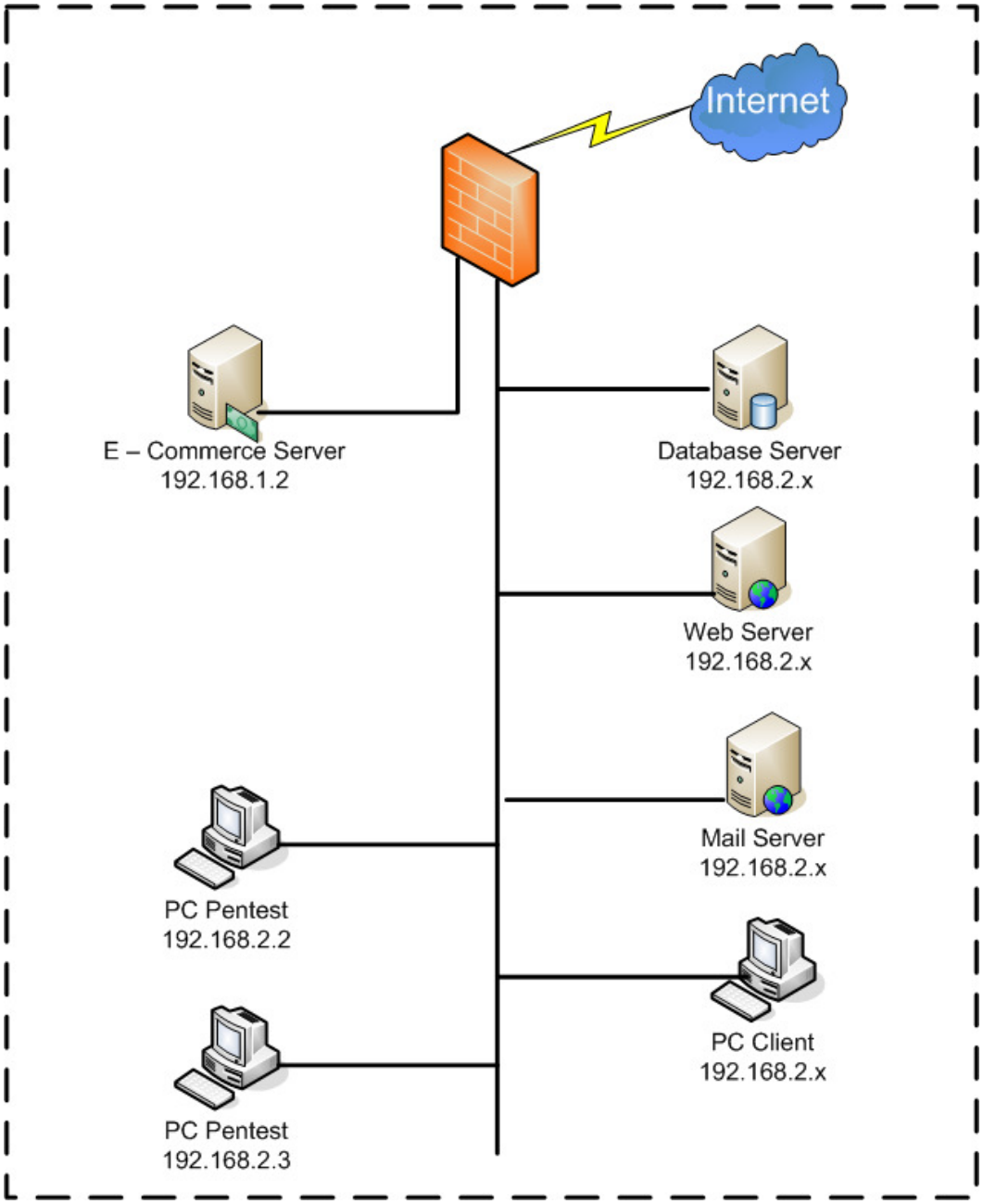
3. Xác định chính xác tên tài khoản Administrator của Server.*Thực hiện được ý này đội thi sẽ nhân được……điểm.*

4. Xác định chính xác các Port đang được mở trên Server (Sai 1 port cũng không được tính điểm). *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

3. Quy định dành cho thi sinh:

- Ngoài hệ thống đang được cài đặt và cấu hình sẵn thì thí sinh không được phép cài đặt thêm các ứng dụng mới nào trên cả client và server.
- Thí sinh không được phép đưa usb, CD, DVD, các thiết bị ngoại vi khác vào hệ thống.
- Thí sinh không được sử dụng điện thoại di động, hay các thiết bị ngoại vi khác trong thời gian thi.

C. ĐỀ THI THỨ BA:



D. Mô tả hệ thống:

Cho một hệ thống mạng như hình vẽ trên. Hệ thống mạng bao gồm:

- Một Firewall
- Một Web Server
- Một Mail Server
- Một Database Server

- Một E-Commerce Server
- Một máy PC client
- Hai máy Pentest dành cho thí sinh sử dụng.
- Ứng dụng web đang chạy trên webserver có địa chỉ: http://vnisa.vn
- Trên các máy client có cài đặt sẵn một số công cụ và có 1 thư mục chức các shell code cho thí sinh lựa chọn để sử dụng khi cần thiết.

Một số thông tin về ứng dụng:

- Ứng dụng web là một website Online Banking Demo của một ngân hàng. Thí sinh có 3 tài khoản để đăng nhập vào để sử dụng các tính năng của Online Banking:
  User1: jv pass: jv789
  User2: jc pass: jc789
  User3: jm pass: jm789

E. **Yêu cầu của đề thi:**

Phần 1: Điều tra thông tin hệ thống

- Hãy xác định địa chỉ IP chính xác của các Server và Client trên hệ thống mạng đã cho. (Trừ 2 máy Pentest và E-commerce Server) – *Mỗi địa chỉ IP chính xác thí sinh được …… điểm.*
- Hãy xác định chính xác các port tương ứng với dịch vụ đang chạy trên mỗi Server. – *Mỗi địa chỉ Port-service chính xác thí sinh được …… điểm.*

Phần 2: Liệt kê các điểm yếu trên hệ thống

- Hãy cho biết điểm yếu an toàn thông tin của sơ đồ thiết kế mạng trên. Giải thích vì sao ? Và đề xuất kỹ thuật khắc phục. – *Mỗi ý trả lời chính xác thí sinh sẽ được …. điểm.*

- Hãy cho biết phiên bản hệ điều hành của Web Server và chỉ ra ít nhất 2 điểm yếu trên Web Server. - *Trả lời chính xác thí sinh sẽ được …. điểm.*

Phần 3: Xác định lỗ hổng trên ứng dụng Web

- Khai thác các lỗ hổng trên ứng dụng web tại địa chỉ http://vnisa.vn . (Chú thích: Gợi ý đó là một số các lỗ hổng cơ bản như: SQL Injection, XSS, Authorization Failure,…) .

- Mỗi lỗ hổng tìm ra được chính xác (phải chứng minh sự tồn tại) thí sinh sẽ được …. điểm.

- Đề xuất qua về phương án có thể khắc phục được cho lỗ hổng thí sinh sẽ được…..điểm.

Phần 4: Xâm nhập máy chủ

Thí sinh tìm cách xâm nhập vào máy chủ WebServer để thực hiện một số yêu cầu sau:

5. Upload được file có dạng Tendoi.txt vào thư mục www của máy chủ web.(Test *http://192.168.2.x/tendoi.txt* .). *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

6. Xác định chính xác tên của các tài khoản trên Server. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

7. Xác định chính xác tên tài khoản Administrator của Server. *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

8. Từ việc xâm nhập được Web Server hãy xác định chính xác các Port đang được mở trên WebServer (Sai 1 port cũng không được tính điểm). *Thực hiện được ý này đội thi sẽ nhân được……điểm.*

F. Quy định dành cho thi sinh:

- Ngoài hệ thống đang được cài đặt và cấu hình sẵn thì sinh không được phép cài đặt thêm các ứng dụng mới nào trên cả client và server.
- Thí sinh không được phép đưa usb, CD, DVD, các thiết bị ngoại vi khác vào hệ thống.
- Thí sinh không được sử dụng điện thoại di động, hay các thiết bị ngoại vi khác trong thời gian thi.

D. ĐỀ THI THỨ TƯ:

Hai đội được cấp 2 hệ thống máy mạng bao gồm các chủ, các máy client như sau:

- Có 3 máy chủ: Trong đó bao gồm 1 máy chủ web, 1 máy chủ FTP, 1 máy chủ không xác định.
- Có 3 máy client dùng cho thí sinh thực hiện bài thi (trên các máy clientcó sẵn một số công cụ, tài nguyên) – trên các máy client này có một số máy ảo chạy Backtrack 5.
- Dải IP của đội là từ 192.168.0. – 192.168.0.
- Tài khoản của Backtrack và Nessus trên BT5 là:
  user: root
  pass: toor

Nhiệm vụ của 2 đội là tấn công và xâm nhập hệ thống máy tính của lẫn nhau:

I. Điều tra thông tin hệ thống đích (mỗi ý 10điểm)

Sinh viên phải trả lời các câu hỏi sau:

1) Hãy xác định các máy chủcủa đối phương đangchạy hệ điều hành gì và phiên bản sử dụng ?*(Phải đầy đủ thông tin đủ 3 máy chủ mới được tính điểm)*

2) Các dịch vụ và port đang chạy trên hệ điều hành máy chủ là những dịch vụgì ?*(Phải đầy đủ thông tin đủ 3 máy chủ mới được tính điểm)*

II. Liệt kê các điểm yếu của hệ thống (mỗi ý 10 điểm)

1) Liệt kê các điểm yếu trên các máy chủ ? (3 điểm yếu, lỗ hổng trở lên)(*với mỗi máy chủ được tính là 1 ý*)

III. Khai thác các điểm yếu của hệ thống (mỗi ý 10điểm)*(Chỉ khai thác trên máy chủ FTP)*

1) Dựa vào điểm yếu nào mà có thể khai thác được hệ thống ?
2) Tạo một tập tin tại ổ địa C:\ với tên đội của mình.Ví dụ đội XXX dự thì sẽ tạo tập tin C:\doiXXX.txt.

IV. Leo thang đặc quyền (20 điểm)*(Chỉ khai thác trên máy chủ FTP)*

1) Bằng bất cứ công cụ hay kỹ thuật nào để chiếm toàn quyền máy và tạo một tài khoản với tên đội mình trên hệ thống và thuộc nhóm Administrators.

Ví dụ: đội XXX sẽ tạo tài khoản là userXXX và userXXX này phải nằm trong nhóm Administrators.

V. Tấn công vào ứng dụng Web

Hai đội có nhiệm vụ tấn công vào hệ thống website của nhau theo các ý trong đề thi như sau: *(Chú ý trong phần này thí sinh không được sử dụng các công cụ, phần mềm trên Backtrack 5)*

V.1. Khai thác lỗi bảo mật SQL Injection trên ứng dụng web.

Level 1 (10 điểm)– *sinh viên phải trả lời đủ ý mới tính điểm*

Các bạn hãy khai thác lỗi và trả lời các câu hỏi sau:

1) Mật khẩu của level1 là gì ?

2) Trình bày phương pháp lấy mật khẩu level1 ?

Level 2 (20 điểm) - *sinh viên phải trả lời đủ ý mới tính điểm*

Các bạn hãy khai thác lỗi và trả lời các câu hỏi sau:

1) Tấn công trang đăng nhập level 2 và cho biết mật khẩu của level2 là gì ? (15 điểm)

2) Trình bày phương pháp lấy mật khẩu level2 ?

Gợi ý:

Sử dụng điều kiện đúng/sai trong câu lệnh SQL để tìm ra mật khẩu level2.Tìm kiếm các hàm xử lý chuỗi trong câu lệnh SQL.

Level 3 (30 điểm) - *sinh viên phải trả lời đủ ý mới tính điểm*

Để phòng tránh lỗi bảo mật SQL Injection.Người phát triển đã sử dụng hàm base64_encode và base64_decode trong mã lệnh của phần đăng nhập level3.Tuy nhiên, việc phòng chống này là không toàn diện và vẫn bị lỗi. Các bạn hãy khai thác lỗi và trả lời các câu hỏi sau:

1) Tấn công trang đăng nhập level 3 và cho biết mật khẩu của level3 là gì ?

2) Trình bày phương pháp lấy mật khẩu level3

V.2. Khai thác lỗi bảo mật Upload file trên ứng dụng web.

Level 1 (10 điểm)

Tình huống:

Một ứng dụng Web chỉ cho phép tải tập tin hình ảnh (*.gif) lên hệ thống bằng cách sử dụng mã JavaScript để ngăn chặn những tập tin không được phép.Tuy nhiên, việc lập trình này có thể bị kẻ tấn công vượt qua và tải các tập tin độc hại cho hệ thống.

Nhiệm vụ:

Đội chơi có nhiệm vụ có nhiệm vụ tấn công ứng dụng và tải một tập tin (*.php) có tên đội mình. Ví dụ: đội XXX sẽ có nhiệm vụ tải tập tin doiXXX.php.

Lưu ý:

Tập tin được tải lên nằm tại thư mục uploads đồng cấp với thư mục level1.

Level 2 (20 điểm)

Tình huống:

Cho ứng dụng tương tự như level1.Người lập trình đã nhận thức được việc sử dụng mã JavaScript để ngăn chặn như level1 là thất bại.Vì vậy người lập trình đã thêm đoạn mã kiểm tra kiểu tập tin tải lên để tránh kẻ tấn công tải lên những tập tin độc hại cho hệ thống.Tuy nhiên, việc lập trình thêm mã kiểm tra kiểu tập tin tải cũng thất bại.

Nhiệm vụ:

Đội chơi có nhiệm vụ có nhiệm vụ tấn công ứng dụng và tải một tập tin (*.php) có tên đội mình. Ví dụ: đội XXX sẽ có nhiệm vụ tải tập tin doiXXX.php.

Lưu ý:

Tập tin được tải lên nằm tại thư mục uploads đồng cấp với thư mục level2.

Level 3 (20 điểm)

Tình huống:

Việc kiểm tra kiểu tập tin tải lên của người lập trình cũng thất bại ở level2. Do vậy, người lập trình đã sửa lại mã lập trình cho an toàn hơn bằng cách kiểm tra nội dung tập tin. Tức là, người lập trình đã sử dụng mã lập trình kiểm tra nội dung của tập tin tải lên thực sự là nội dung của ảnh (*.gif hoặc *.jpg) thì mới cho phép tải lên.Ngược lại, tập tin có nội dung không phù hợp thì không được phép.Tuy nhiên, việc lập trình này của người phát triển cũng thất bại và cũng cho phép kẻ tấn công có thể tải lên những tập tin độc hại.

Nhiệm vụ:

Đội chơi có nhiệm vụ có nhiệm vụ tấn công ứng dụng và tải một tập tin (*.php) có tên đội mình. Ví dụ: đội XXX sẽ có nhiệm vụ tải tập tin doiXXX.php.

Lưu ý:

Tập tin được tải lên nằm tại thư mục uploads đồng cấp với thư mục level3.

Level 4 (30 điểm)

Tình huống:

Người lập trình đã nhận biết được cách lập trình như thế nào là triệt để bằng cách sửa mã lệnh kiểm tra không cho phép tải bất kỳ tập tin *.php,*.php3, *.php4 nào được tải lên hệ thống.

Câu hỏi:

Level 4 này có bị khai thác tải các tập tin độc hại lên được không ? Vì sao ?

Tình huống như thế nào thì kẻ tấn công có thể khai thác được lỗ hổng tải tập tin ?

Lưu ý:

Tập tin được tải lên nằm tại thư mục uploads đồng cấp với thư mục level4.

Final (30 điểm)

Tất cả các tập tin có khả năng thực thi trên hệ thống (*.php) đều bị máy chủ web ngăn chặn không cho phép thực thi. Hãy rà soát lại tất cả các level đã làm và thử vượt qua sự truy cản này.