With Metasploit:

I first conducted an nmap scan and saw that port 80 was open, and that the service the web server was running on was Microsoft IIS 6.0. There is an ScStoragePathFromUrl exploit associated with the service (https://www.rapid7.com/db/modules/exploit/windows/iis/iis_webdav_scstoragepathfromurl). I gained a meterpreter session, and migrated to a process with NT/Authority system. I then used exploit suggester for priv esc, and used the track_popup exploit. In order for a session to be created / to start, I also needed to make sure the local host was correct (i.e. the tun0 localhost, not the eth0).