Spawning a TTY Shell

Peleus

Often during pen tests you may obtain a shell without having tty, yet wish to interact further with the system. Here are some commands which will allow you to spawn a tty shell. Obviously some of this will depend on the system environment and installed packages.

Shell Spawning

- `python -c 'import pty; pty.spawn("/bin/sh")'`
- `echo os.system('/bin/bash')`
- `/bin/sh -i`
- `perl —e 'exec "/bin/sh";'`
- `perl: exec "/bin/sh";`
- `ruby: exec "/bin/sh"`
- `lua: os.execute('/bin/sh')`
- (From within IRB)
  `exec "/bin/sh"`

- (From within vi)
```
:!bash
```

- (From within vi)
```
:set shell=/bin/bash:shell
```

- (From within nmap)
```
!sh
```

Many of these will also allow you to escape jail shells. The top 3 would be my most successful in general for spawning from the command line.

Filed Under: Basic Information
Tagged With: shell, shell spawning, tty