5. Attempt Command Injection

```
alert tcp any any -> $HOME_NET 80 (\
    msg: "Attempt Command Injection detected - /files";\
    flow:to_server; content:"POST", nocase;\
    content:"file_name=", nocase;\
    pcre:"/(\%26|%2A|%3B|%3C|%3E|%3F|%60|%7C)/i";\
    pcre:"/(CMD|SH|ECHO|NC|WGET|CD|LS|DIR|WHOAMI|ID|IPCONFIG|CAT|TAIL|HEAD|CHMOD)/i";\
    sid: 1000035;\
)
```

```
pcre:"/(CMD|BASH|SH|POWERSHELL|ECHO|NC|WGET|UNAME|CD|LS|DIR|WHOAMI|IFCONFIG|ID|HOSTNAME|IP
CONFIG|CAT|TAIL|HEAD|CHMOD)/i";\
```