# Sample *Snort* Signature

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139
  flow:to_server,established
content:"|eb2f 5feb 4a5e 89fb 893e 89f2|"
msg:"EXPLOIT x86 linux samba overflow"
reference:bugtraq,1816
reference:cve,CVE-1999-0811
classtype:attempted-admin
```

# Sample *Snort* Signature

-
  ```
  alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
                                 $HTTP_PORTS
     (msg:"WEB-CGI finger access";
      flow:to_server,established;
      uricontent:"/finger"; nocase;
      reference:arachnids,221;
      reference:cve,1999-0612;
      reference:nessus,10071;
      classtype:attempted-recon;
      sid:839; rev:7;)
  ```

# Snort Botnet Command-and-Control Rule

- alert ip $HOME_NET any -> [206.59.139.195,207.114.175.51,207.126.115.205,207.126.115.219,207.126.162.236,207.126.162.237,207.150.167.55,207.162.194.151,207.179.120.238,207.182.240.68,207.192.72.43,207.192.72.99,207.192.73.110,207.210.208.16,207.44.152.199,207.44.180.227,207.44.184.225,207.45.69.69,208.100.20.83,208.100.20.90,208.100.23.100,208.100.38.15,208.110.65.135,208.110.69.227,208.111.34.13,208.111.35.75,208.127.19.151,208.146.35.105,208.146.35.106,208.167.236.6,208.167.237.120,208.185.80.72,208.185.80.74,208.185.80.85,208.185.80.87,208.185.81.205,208.185.81.237,208.185.81.243,208.185.82.128,208.185.92.26,208.185.92.31,208.20.225.248,208.27.69.193,208.51.40.10,208.51.40.2,208.53.146.4,208.53.146.6,208.53.148.111,208.53.148.254,208.53.148.8,208.53.150.43,208.53.150.44,208.53.163.194,208.53.172.67,208.53.175.92,208.53.181.86,208.67.249.244,208.68.94.62,208.72.157.63,208.77.191.41] any (msg:"ET DROP Known Bot C&C Server Traffic (group 5) "; reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 3600, count 1; classtype:trojan-activity; sid:2404004; rev:1660;)