

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;)
```

Sample Snort *Vulnerability* Signature

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
                                     $HTTP_PORTS
uricontent: ".ida?"; nocase; dsize: > 239;
flags:A+
msg:"Web-IIS ISAPI .ida attempt"
reference:bugtraq,1816
reference:cve,CAN-2000-0071
classtype:attempted-admin
```