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
```

MarketPlace | About | Services | FAQ | Blog | Contacts

WabiSabiLabi

CLOSER TO ZERØ RISK

Home page ▸ Current bids

Sign in

Username

Password

Sign in

New user? Sign up here

News

PRESS RELEASE 03/07/2007
Finally a Marketplace Site for Security Research

Current bids | MarketPlace history

4 items found, displaying all items. Page **1**

Code	Time to live	Title	System	Offer type	Bid	
ZD-00000007	9d 13h 26m	Local Linux kernel memory leak	Linux	Bidding	600€	1 bid(s)
ZD-00000005	9d 13h 26m	Yahoo! Messenger 8.1 remote buffer overflow	Windows XP	Bidding	2,000€	0 bid(s)
ZD-00000004	9d 13h 26m	Squirrelmail GPG Plugin Command Execution	Web application	Bidding Buy now at	600€ 1,750€	1 bid(s)
ZD-00000008	10d 13h 26m	MKPortal SQL injection	Web application	Bidding Buy now at	500€ 800€	0 bid(s)

Current bids | MarketPlace history

4 items found, displaying all items. Page **1**

Code	Time to live	Title	System	Offer type	Bid	
ZD-00000007	9d 13h 26m	Local Linux kernel memory leak	Linux	Bidding	600€	1 bid(s)
ZD-00000005	9d 13h 26m	Yahoo! Messenger 8.1 remote buffer overflow	Windows XP	Bidding	2,000€	0 bid(s)
ZD-00000004	9d 13h 26m	Squirrelmail GPG Plugin Command Execution	Web application	Bidding Buy now at	600€ 1,750€	1 bid(s)
ZD-00000008	10d 13h 26m	MKPortal SQL injection	Web application	Bidding Buy now at	500€ 800€	0 bid(s)

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;)
  ```
  ```

1 day of “crud” seen at ICSI (155K times)

active-connection-reuse	DNS-label-len-gt-pkt	HTTP-chunked-multipart	possible-split-routing
bad-Ident-reply	DNS-label-too-long	HTTP-version-mismatch	SYN-after-close
bad-RPC	DNS-RR-length-mismatch	illegal-%-at-end-of-URI	SYN-after-reset
bad-SYN-ack	DNS-RR-unknown-type	inappropriate-FIN	SYN-inside-connection
bad-TCP-header-len	DNS-truncated-answer	IRC-invalid-line	SYN-seq-jump
base64-illegal-encoding	DNS-len-lt-hdr-len	line-terminated-with-single-CR	truncated-NTP
connection-originator-SYN-ack	DNS-truncated-RR-rdlength	malformed-SSH-identification	unescaped-%-in-URI
data-after-reset	double-%-in-URI	no-login-prompt	unescaped-special-URI-char
data-before-established	excess-RPC	NUL-in-line	unmatched-HTTP-reply
too-many-DNS-queries	FIN-advanced-last-seq	POP3-server-sending-client-commands	window-recision
DNS-label-forward-compress-offset	fragment-with-DF		