

Attacker IP: 94.156.177.0/24

Target IP: 62.72.**.51

Total Attack > 50

Attack Time: 2024-09-06-2024-09-14

Attack Type: Mail Cracking & Relay attempt

Block: /24 subnet | > 5 IP attack from the subnet

```
[root@gl exin]# cat reject* | grep -w 94.156.177
2024-09-06 06:30:19 Hs(WIN-7N1FIECLGIC.domain) [94.156.177.63] F=<test@my.id> rejected RCPT <grantgrayzxp@outlook.com>: Rejected relay attempt: '94.156.177.63' From: 'test@my.id' To: 'grantgrayzxp@outlook.com'
2024-09-07 01:37:54 Hs(WIN-7N1FIECLGIC.domain) [94.156.177.51] F=<test@my.id> rejected RCPT <raqqush1@outlook.com>: Rejected relay attempt: '94.156.177.51' From: 'test@my.id' To: 'raqqush1@outlook.com'
2024-09-07 22:05:30 Hs(WIN-7N1FIECLGIC) [94.156.177.132] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-09 21:55:37 Hs(WIN-7N1FIECLGIC) [94.156.177.37] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-10 07:41:58 Hs(WIN-7N1FIECLGIC) [94.156.177.52] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-11 07:08:06 Hs(WIN-7N1FIECLGIC.domain) [94.156.177.63] F=<test@my.id> rejected RCPT <grantgrayzxp@outlook.com>: Rejected relay attempt: '94.156.177.63' From: 'test@my.id' To: 'grantgrayzxp@outlook.com'
2024-09-13 20:44:56 Hs(WIN-7N1FIECLGIC) [94.156.177.75] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-13 22:52:54 Hs(WIN-7N1FIECLGIC) [94.156.177.61] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-13 23:47:24 Hs(WIN-7N1FIECLGIC) [94.156.177.77] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
2024-09-14 10:25:37 Hs(WIN-7N1FIECLGIC) [94.156.177.10] rejected MAIL <spamer@iscali.it>: Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
```