

ALERTS

[**][1:498:6] ATTACK-RESPONSES id check returned root [**]

[Classification: Potentially Bad Traffic] [Priority: 2]

03/07-13:19:48.833805 192.168.2.128:443 -> 192.168.2.7:51763

TCP TTL:64 TOS:0x10 ID:48821 IpLen:20 DgmLen:112 DF

AP Seq: 0x3AF2952E Ack: 0x4C0220AD Win: 0x2086 TcpLen: 32

TCP Options (3) => NOP NOP TS: 775942993 11010991

[**][1:498:6] ATTACK-RESPONSES id check returned root [**]

[Classification: Potentially Bad Traffic] [Priority: 2]

03/07-13:19:50.233117 192.168.2.128:443 -> 192.168.2.7:51763

TCP TTL:64 TOS:0x10 ID:48891 IpLen:20 DgmLen:112 DF

AP Seq: 0x3AF2960E Ack: 0x4C0220BB Win: 0x2086 TcpLen: 32

TCP Options (3) => NOP NOP TS: 775944393 11014588