10/28/2022-14:53:04.274275 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:07.286239 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:16.320517 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:19.326094 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:21.331732 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:28.346118 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:37.370466 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:41.382094 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:44.391476 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:52.417906 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:53:53.420141 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:54:04.443545 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:55:52.343651 [\*\*] [1:2001219:20] ET SCAN Potential SSH Scan [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:56856 -> 192.168.28.53:22

10/28/2022-14:55:52.343651 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:56856 -> 192.168.28.53:22

10/28/2022-14:55:52.346619 [\*\*] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [\*\*] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.28.55:56854 -> 192.168.28.53:22

10/28/2022-14:56:49.511408 [\*\*] [1:2001219:20] ET SCAN Potential SSH Scan [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:41248 -> 192.168.28.53:22

10/28/2022-14:56:49.511408 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:41248 -> 192.168.28.53:22

10/28/2022-14:56:49.513626 [\*\*] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [\*\*] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.28.55:41228 -> 192.168.28.53:22

10/28/2022-14:56:57.082775 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:13.115650 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:21.128256 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:24.129723 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:27.134338 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:28.138483 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:29.140150 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:41.154243 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:44.159803 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:57:54.178806 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:17.215099 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:22.224260 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:23.228050 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:24.231592 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:37.253493 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:41.259829 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:44.275856 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:48.285855 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:58:57.294401 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:59:12.316672 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:59:30.346120 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:59:42.375732 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:59:46.388577 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-14:59:49.397835 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:00:17.460869 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:00:33.489091 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:01:28.601057 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:08.722095 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:16.769603 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:19.822784 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:33.884182 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:40.932935 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:43.933901 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:49.985041 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:02:52.989632 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:03:13.017372 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:03:22.012601 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:03:23.019281 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:05:14.260378 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:05:21.274531 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:05:44.368210 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:08.420212 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:16.431585 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:30.451333 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:33.464711 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:35.469021 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:40.474783 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:45.481109 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:48.488580 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:06:56.500555 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:07:04.521547 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:07:16.538423 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:07:20.544025 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:11.666382 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:14.678257 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:16.672600 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:19.670418 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:20.680396 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:31.729322 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:32.777670 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:37.700111 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:47.719310 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:08:52.726259 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:02.527010 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:39938 -> 127.0.0.1:6379

10/28/2022-15:09:04.746116 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:07.754406 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:12.765224 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:28.789902 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:36.802301 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:40.512251 [\*\*] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.28.55:55944 -> 192.168.28.53:3306

10/28/2022-15:09:40.542219 [\*\*] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.28.55:37952 -> 192.168.28.53:5432

10/28/2022-15:09:40.609596 [\*\*] [1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:60464 -> 192.168.28.53:5904

10/28/2022-15:09:40.646155 [\*\*] [1:2002910:6] ET SCAN Potential VNC Scan 5800-5820 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:35116 -> 192.168.28.53:5811

10/28/2022-15:09:40.656321 [\*\*] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.28.55:38014 -> 192.168.28.53:1521

10/28/2022-15:09:40.651085 [\*\*] [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.28.55:47832 -> 192.168.28.53:1433

10/28/2022-15:09:44.800206 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:46.850951 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:50400

10/28/2022-15:09:46.888614 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40246 -> 192.168.28.53:3000

10/28/2022-15:09:46.888614 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40246 -> 192.168.28.53:3000

10/28/2022-15:09:46.888614 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40236 -> 192.168.28.53:3000

10/28/2022-15:09:46.888614 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40236 -> 192.168.28.53:3000

10/28/2022-15:09:46.903479 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40264 -> 192.168.28.53:3000

10/28/2022-15:09:46.903479 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40264 -> 192.168.28.53:3000

10/28/2022-15:09:46.905425 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40274 -> 192.168.28.53:3000

10/28/2022-15:09:46.905425 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40274 -> 192.168.28.53:3000

10/28/2022-15:09:46.911697 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40292 -> 192.168.28.53:3000

10/28/2022-15:09:46.911697 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40292 -> 192.168.28.53:3000

10/28/2022-15:09:46.910553 [\*\*] [1:2009358:6] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40282 -> 192.168.28.53:3000

10/28/2022-15:09:46.910553 [\*\*] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [\*\*] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.28.55:40282 -> 192.168.28.53:3000

10/28/2022-15:09:48.820821 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:09:52.829835 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:10:22.857855 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:00.327521 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:00.329500 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:02.331415 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:05.333213 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:14.361800 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:14.362333 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:15.360128 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:21.385517 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:23.396448 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:26.408406 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:27.413360 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:29.426286 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:36.467289 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:42.487350 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:43.493771 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:45.507988 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:45.516787 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:49.527073 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:53.532159 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:55.826996 [\*\*] [1:2001219:20] ET SCAN Potential SSH Scan [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:33027 -> 192.168.28.53:22

10/28/2022-15:13:55.826996 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:33027 -> 192.168.28.53:22

10/28/2022-15:13:57.534031 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38857 -> 192.168.28.53:22

10/28/2022-15:13:58.570504 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:13:59.417090 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:43339 -> 192.168.28.53:22

10/28/2022-15:13:59.576483 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:00.621280 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:01.165183 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:41887 -> 192.168.28.53:22

10/28/2022-15:14:02.923125 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:40167 -> 192.168.28.53:22

10/28/2022-15:14:03.647501 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:04.513855 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:41497 -> 192.168.28.53:22

10/28/2022-15:14:05.654161 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:05.998622 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46137 -> 192.168.28.53:22

10/28/2022-15:14:07.654267 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:08.225009 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:36453 -> 192.168.28.53:22

10/28/2022-15:14:09.671728 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:09.851740 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:39069 -> 192.168.28.53:22

10/28/2022-15:14:11.442855 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38219 -> 192.168.28.53:22

10/28/2022-15:14:13.176340 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:42533 -> 192.168.28.53:22

10/28/2022-15:14:14.834321 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:34769 -> 192.168.28.53:22

10/28/2022-15:14:16.549519 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46033 -> 192.168.28.53:22

10/28/2022-15:14:18.292638 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:33885 -> 192.168.28.53:22

10/28/2022-15:14:19.856270 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46433 -> 192.168.28.53:22

10/28/2022-15:14:21.569086 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:32905 -> 192.168.28.53:22

10/28/2022-15:14:23.291457 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:43245 -> 192.168.28.53:22

10/28/2022-15:14:24.804441 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38781 -> 192.168.28.53:22

10/28/2022-15:14:26.356205 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:43447 -> 192.168.28.53:22

10/28/2022-15:14:27.883544 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:35139 -> 192.168.28.53:22

10/28/2022-15:14:29.554927 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:33675 -> 192.168.28.53:22

10/28/2022-15:14:31.244207 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:44909 -> 192.168.28.53:22

10/28/2022-15:14:32.878929 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:35159 -> 192.168.28.53:22

10/28/2022-15:14:34.561800 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46753 -> 192.168.28.53:22

10/28/2022-15:14:36.276048 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:42921 -> 192.168.28.53:22

10/28/2022-15:14:36.790560 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:37.705271 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:33241 -> 192.168.28.53:22

10/28/2022-15:14:37.781032 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:39.328169 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:45717 -> 192.168.28.53:22

10/28/2022-15:14:40.799621 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:37579 -> 192.168.28.53:22

10/28/2022-15:14:40.809564 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:41.813110 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:42.382623 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:36731 -> 192.168.28.53:22

10/28/2022-15:14:42.826319 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:43.828881 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46099 -> 192.168.28.53:22

10/28/2022-15:14:43.829538 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:14:45.420012 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:37899 -> 192.168.28.53:22

10/28/2022-15:14:46.907426 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:40497 -> 192.168.28.53:22

10/28/2022-15:14:48.603397 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:45485 -> 192.168.28.53:22

10/28/2022-15:14:50.157017 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:32849 -> 192.168.28.53:22

10/28/2022-15:14:51.689367 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:41611 -> 192.168.28.53:22

10/28/2022-15:14:53.176056 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:37745 -> 192.168.28.53:22

10/28/2022-15:14:54.717336 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:46553 -> 192.168.28.53:22

10/28/2022-15:14:56.262779 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38061 -> 192.168.28.53:22

10/28/2022-15:14:57.916338 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:44971 -> 192.168.28.53:22

10/28/2022-15:14:59.607308 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:35949 -> 192.168.28.53:22

10/28/2022-15:15:00.988227 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38431 -> 192.168.28.53:22

10/28/2022-15:15:02.398804 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:35411 -> 192.168.28.53:22

10/28/2022-15:15:03.765747 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:44401 -> 192.168.28.53:22

10/28/2022-15:15:05.376217 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:40019 -> 192.168.28.53:22

10/28/2022-15:15:06.930872 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:38415 -> 192.168.28.53:22

10/28/2022-15:15:08.672050 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:36235 -> 192.168.28.53:22

10/28/2022-15:15:27.926398 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:15:36.950229 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:15:46.974810 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:15:48.039202 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:47408 -> 192.168.28.53:5601

10/28/2022-15:16:00.057696 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:47408 -> 192.168.28.53:5601

10/28/2022-15:16:12.026107 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:16:15.025104 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:16:22.649951 [\*\*] [1:2001219:20] ET SCAN Potential SSH Scan [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:49346 -> 192.168.28.53:22

10/28/2022-15:16:22.649951 [\*\*] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.28.55:49346 -> 192.168.28.53:22

10/28/2022-15:16:22.652854 [\*\*] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [\*\*] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.28.55:49338 -> 192.168.28.53:22

10/28/2022-15:16:33.049535 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:16:34.060021 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:16:47.077831 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:16:48.081857 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:02.112306 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:03.112005 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:03.706025 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:34808 -> 192.168.28.53:5601

10/28/2022-15:17:05.120582 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:07.506229 [\*\*] [1:2006546:9] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack [\*\*] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.28.55:36098 -> 192.168.28.53:22

10/28/2022-15:17:13.132316 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:29.162190 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:53.213310 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:54.219044 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:55.222428 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:17:58.226411 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:18:01.230872 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:18:01.997579 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:39784 -> 127.0.0.1:6379

10/28/2022-15:18:02.033644 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:39786 -> 127.0.0.1:6379

10/28/2022-15:18:23.269274 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:18:36.298422 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:19:10.372723 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:19:41.406264 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:19:41.923087 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:34808 -> 192.168.28.53:5601

10/28/2022-15:19:43.466304 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56712 -> 192.168.28.53:5601

10/28/2022-15:19:59.455827 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:00.460661 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:04.478933 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:04.478979 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:05.482244 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:07.490622 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:11.504461 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:11.674424 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56726 -> 192.168.28.53:5601

10/28/2022-15:20:13.510199 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:23.524021 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:24.533146 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:33.542080 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:20:43.553839 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:21.637143 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:23.650150 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:25.654597 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:25.794759 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56712 -> 192.168.28.53:5601

10/28/2022-15:21:27.347614 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:34808 -> 192.168.28.53:5601

10/28/2022-15:21:28.802745 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56726 -> 192.168.28.53:5601

10/28/2022-15:21:29.665285 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:30.671723 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:31.672815 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:33.653542 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56712 -> 192.168.28.53:5601

10/28/2022-15:21:35.044971 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:34808 -> 192.168.28.53:5601

10/28/2022-15:21:37.683623 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:41.695249 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:21:53.714368 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:01.729467 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:02.730720 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:11.747407 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:11.747481 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:14.748531 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:15.747613 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:24.755082 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:27.759564 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:33.761089 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:40.769799 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:22:56.805559 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:04.817902 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:06.822193 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:09.824324 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:12.828740 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:14.833863 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:21.855640 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:28.873241 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:32.879845 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:23:52.896760 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:24:09.925712 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:24:16.923992 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:24:41.969314 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:02.245510 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:39752 -> 127.0.0.1:6379

10/28/2022-15:25:21.039184 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:21.044125 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:22.040107 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:23.042553 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:29.048128 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:40.063104 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:44.073303 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:56.092183 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:25:57.093156 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:00.100274 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:53982 -> 192.168.28.53:5601

10/28/2022-15:26:23.144321 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:23.144381 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:39.164484 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:46.186359 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:50.182062 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:26:57.201677 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:27:45.683065 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:44589 -> 192.168.28.53:3000

10/28/2022-15:27:45.683065 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:44589 -> 192.168.28.53:3000

10/28/2022-15:27:46.894061 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:33821

10/28/2022-15:27:51.819327 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:42313 -> 192.168.28.53:3000

10/28/2022-15:27:51.819327 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:42313 -> 192.168.28.53:3000

10/28/2022-15:27:53.029683 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:39255

10/28/2022-15:27:54.634843 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:38511 -> 192.168.28.53:3000

10/28/2022-15:27:54.634843 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:38511 -> 192.168.28.53:3000

10/28/2022-15:27:55.845040 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:34089

10/28/2022-15:27:56.303048 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:01.270007 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:33085 -> 192.168.28.53:3000

10/28/2022-15:28:01.270007 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:33085 -> 192.168.28.53:3000

10/28/2022-15:28:02.484036 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:45839

10/28/2022-15:28:04.262379 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43527 -> 192.168.28.53:3000

10/28/2022-15:28:04.262379 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43527 -> 192.168.28.53:3000

10/28/2022-15:28:05.320048 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:05.472167 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:39203

10/28/2022-15:28:06.854626 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:35857 -> 192.168.28.53:3000

10/28/2022-15:28:06.854626 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:35857 -> 192.168.28.53:3000

10/28/2022-15:28:08.064472 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:43319

10/28/2022-15:28:09.344467 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:42411 -> 192.168.28.53:3000

10/28/2022-15:28:09.344467 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:42411 -> 192.168.28.53:3000

10/28/2022-15:28:09.347788 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:09.351391 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:10.555628 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:38997

10/28/2022-15:28:11.353080 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:12.362631 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:12.590472 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:33831 -> 192.168.28.53:3000

10/28/2022-15:28:12.590472 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:33831 -> 192.168.28.53:3000

10/28/2022-15:28:13.800477 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:40441

10/28/2022-15:28:14.367834 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:15.912866 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:39419 -> 192.168.28.53:3000

10/28/2022-15:28:15.912866 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:39419 -> 192.168.28.53:3000

10/28/2022-15:28:17.125108 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:33237

10/28/2022-15:28:18.776657 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43139 -> 192.168.28.53:3000

10/28/2022-15:28:18.776657 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43139 -> 192.168.28.53:3000

10/28/2022-15:28:19.985380 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:38731

10/28/2022-15:28:26.394271 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:33.426081 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:43.475422 [\*\*] [1:2221028:1] SURICATA HTTP Host header invalid [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43753 -> 192.168.28.53:3000

10/28/2022-15:28:43.475422 [\*\*] [1:2221045:1] SURICATA HTTP Unexpected Request body [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.55:43753 -> 192.168.28.53:3000

10/28/2022-15:28:44.685272 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:38953

10/28/2022-15:28:47.443126 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:51.448472 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:28:57.470970 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:29:12.508544 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:29:16.509445 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:29:23.523090 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:29:54.556780 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:30:08.585996 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:30:17.608152 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:30:22.615214 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:30:24.621161 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:13.715121 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:20.717426 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:22.732272 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:25.749082 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:27.750043 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:28.752077 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:36.766260 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:37.774547 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:31:48.798120 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:07.833112 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:08.834465 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:09.829042 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:11.840269 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:13.836470 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:14.857742 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:46555

10/28/2022-15:32:23.858927 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:24.860042 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:25.861958 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:28.122452 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:34401

10/28/2022-15:32:30.181032 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:43159

10/28/2022-15:32:32.586318 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:42679

10/28/2022-15:32:34.436169 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:40047

10/28/2022-15:32:36.473184 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:46281

10/28/2022-15:32:38.688153 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:34275

10/28/2022-15:32:41.056215 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:36143

10/28/2022-15:32:42.916176 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:43.270424 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:37061

10/28/2022-15:32:45.919519 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:48.929902 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:49.057469 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:56726 -> 192.168.28.53:5601

10/28/2022-15:32:50.542300 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:58238 -> 192.168.28.53:5601

10/28/2022-15:32:51.943362 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:53.960416 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:56.963748 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:32:57.966576 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:33:06.969243 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:33:12.980158 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:33:19.987301 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:33:21.992275 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:33:42.147549 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:44215

10/28/2022-15:33:48.027249 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:34:06.743362 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:34653

10/28/2022-15:34:08.069315 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:34:11.323445 [\*\*] [1:2260000:1] SURICATA Applayer Mismatch protocol both directions [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:3000 -> 192.168.28.55:46597

10/28/2022-15:34:13.068320 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:34:17.073647 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:34:24.088241 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:34:44.126398 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:35:29.195327 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:35:54.238137 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:12.260950 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:18.272479 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:23.311254 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:25.318092 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:33.332944 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:41.344371 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:43.352495 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:44.355246 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:45.359366 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:46.361743 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:47.381578 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:48.376541 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:36:49.035947 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:45506 -> 192.168.28.53:5601

10/28/2022-15:37:18.146905 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:37:19.454381 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:21.465471 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:24.474169 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:27.569149 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:37:29.484540 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:29.485120 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:37.649797 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:37:39.495658 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:40.177029 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:37:41.502511 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:37:55.522064 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:38:01.532187 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:38:17.547681 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:38:41.589254 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:38:59.614891 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:38:59.616517 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:02.010187 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:51522 -> 127.0.0.1:6379

10/28/2022-15:39:03.432569 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:39:05.630251 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:06.164713 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:56726

10/28/2022-15:39:14.647799 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:21.662477 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:26.674618 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:29.680218 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:30.681671 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:39:53.721085 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:22.775072 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:26.786507 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:27.788837 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:28.791712 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:33.797941 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:38.810143 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:47.829082 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:40:48.833428 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:04.860403 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:12.879362 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:17.891919 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:21.902183 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:22.902246 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:24.454827 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55566 -> 192.168.28.53:5601

10/28/2022-15:41:24.898360 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:26.039203 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55450 -> 192.168.28.53:5601

10/28/2022-15:41:26.911344 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:27.917259 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:41:40.777505 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55566 -> 192.168.28.53:5601

10/28/2022-15:41:42.298713 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:37248 -> 192.168.28.53:5601

10/28/2022-15:41:46.466686 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55450 -> 192.168.28.53:5601

10/28/2022-15:41:50.646246 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55566 -> 192.168.28.53:5601

10/28/2022-15:41:55.318612 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:37248 -> 192.168.28.53:5601

10/28/2022-15:42:08.119634 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:08.122496 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:14.131025 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:18.141524 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:23.156481 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:32.178153 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:37.186289 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:41.185379 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:42:42.187236 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:43:53.336226 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:43:54.348495 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:40.404839 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:41.408177 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:42.410633 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:47.418663 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:49.422410 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:50.426400 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:51.432227 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:52.437505 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:54.442825 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:55.444035 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:44:57.447256 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:45:13.487471 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:05.572566 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:07.583517 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:09.577377 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:17.592180 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:18.657152 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:19.089570 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:20.029134 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:20.596025 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:22.610145 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:24.130939 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:24.526050 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:25.474396 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:25.612082 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:25.622244 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:26.041411 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:26.534134 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:27.439798 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:27.618668 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:28.689815 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:29.128840 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:30.013223 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:30.605396 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:33.652042 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:36.660726 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:39.667020 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:40.326967 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:41.667092 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:41.765034 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55450 -> 192.168.28.53:5601

10/28/2022-15:46:42.104014 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:42.678194 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:43.708438 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:44.726094 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:48.746688 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:49.751657 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:50.750075 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:51.762024 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:54982 -> 192.168.28.53:5601

10/28/2022-15:46:52.039329 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:52.492486 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:53.152582 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:53.764483 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:56.562067 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:56.856152 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:57.784765 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:58.458460 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:58.701417 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:58.783052 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:46:59.718043 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:46:59.787604 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:02.190117 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:43446 -> 127.0.0.1:6379

10/28/2022-15:47:02.358490 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:02.827334 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:03.682636 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:03.794057 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:03.806554 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:05.281070 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55450 -> 192.168.28.53:5601

10/28/2022-15:47:05.610397 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:05.801186 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:05.952662 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:06.818001 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:06.820479 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:06.916196 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:08.826300 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:13.837382 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:25.401187 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:25.884163 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:26.769058 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:27.558737 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:27.845701 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:27.851606 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:28.788475 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:28.987154 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:34.867939 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:37.872211 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:47:44.241362 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:44.917489 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:45.654235 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:46.788238 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:52.544617 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:52.546137 [\*\*] [1:2221033:1] SURICATA HTTP Request abnormal Content-Encoding header [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.15:55566 -> 192.168.28.53:5601

10/28/2022-15:47:53.095436 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:53.512128 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:54.414838 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:47:55.902666 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:01.990907 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:49850 -> 127.0.0.1:6379

10/28/2022-15:48:02.955267 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:03.345010 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:04.305120 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:15.846842 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:16.240071 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:17.291486 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:18.443509 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:18.869485 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:19.534607 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:22.963747 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:57698 -> 192.168.28.53:5601

10/28/2022-15:48:25.545998 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:57698 -> 192.168.28.53:5601

10/28/2022-15:48:25.953262 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:25.953331 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:25.968808 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:26.475020 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:29.996321 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:40.032834 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:42.008429 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:48:43.582215 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:48:52.843074 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:05.066334 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:05.637597 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:07.057213 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:08.066153 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:13.086218 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:18.464034 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:21.099336 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:29.139023 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:31.291287 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:34.156644 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:35.181070 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:49:44.096159 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:48.840064 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:50.283611 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:55450 -> 192.168.28.53:5601

10/28/2022-15:49:50.491966 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:52.360678 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:49:57.206640 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:09.923892 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:22.642945 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:22.774410 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:23.157565 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:23.273106 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:24.075676 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:24.280420 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:32.303128 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:32.303728 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:33.320639 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:35.945270 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:36.071511 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:36.496798 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:37.410784 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:38.089169 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:41.874971 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:42.027615 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:42.309552 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:43.280343 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:43.706219 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:43.847223 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:44.137139 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:45.129326 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:45.311234 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:45.442778 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:45.879530 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:46.579911 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:46.726361 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55450

10/28/2022-15:50:48.009551 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:48690 -> 192.168.28.53:5601

10/28/2022-15:50:49.318587 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:50:50.371098 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:50:52.382484 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:02.377388 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:42894 -> 192.168.28.53:5601

10/28/2022-15:51:02.632926 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:57362 -> 127.0.0.1:6379

10/28/2022-15:51:02.911355 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:03.482519 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:04.259487 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:04.578967 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:04.772415 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:05.400245 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:06.399969 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:08.888109 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:10.614369 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:11.822439 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:13.121358 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:16.185499 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:19.852579 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:22.657886 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:23.837349 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:25.122299 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:29.075350 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:30.455264 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:31.461772 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:32.463786 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:39.565407 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:41.534765 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:42.130512 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:42.306427 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:51:43.503100 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:44.513069 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:54.520354 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:51:55.038520 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:07.916542 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:08.613311 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:09.543523 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:18.561934 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:20.825274 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:22.566366 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:29.514137 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:31.491120 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:32.366861 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:33.597665 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:33.599089 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:33.919662 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:37.028517 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:38.685097 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:39.598741 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:41.388268 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:55566

10/28/2022-15:52:42.637403 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:52:47.640533 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:53:02.400902 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:57606 -> 127.0.0.1:6379

10/28/2022-15:53:04.667267 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:53:05.676026 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:53:36.711076 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:53:44.950305 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:40656 -> 192.168.28.53:5601

10/28/2022-15:54:02.803245 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:05.810143 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:08.811500 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:09.816683 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:11.609176 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:47542 -> 192.168.28.53:5601

10/28/2022-15:54:12.826292 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:13.830362 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:15.840960 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:16.834671 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:21.877076 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:23.882173 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:29.908403 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:32.910885 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:33.915635 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:43.921355 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:43.921450 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:44.248175 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:44.970657 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:48.977607 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:52.983093 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:54:56.986251 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:02.994092 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:14.025424 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:20.019347 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:20.019367 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:22.755508 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:47542 -> 192.168.28.53:5601

10/28/2022-15:55:22.755594 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:47544 -> 192.168.28.53:5601

10/28/2022-15:55:24.044524 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:27.035321 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:37.046598 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:42.055104 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:47.073430 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:55:47.073467 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:56:04.116145 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:02.008125 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:41910 -> 127.0.0.1:6379

10/28/2022-15:57:05.213673 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:38.285371 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:45.287104 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:46.288087 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:48.310901 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:57:56.723470 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:40656 -> 192.168.28.53:5601

10/28/2022-15:57:56.723545 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:43454 -> 192.168.28.53:5601

10/28/2022-15:58:08.357161 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:05.473452 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:08.481058 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:13.489210 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:17.508523 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:20.515814 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:30.520037 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:36.526138 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:45.540454 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:50.553677 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:53.566363 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:53.568972 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:59.573417 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:59.574833 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-15:59:59.575454 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:00:29.620161 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:00:42.636356 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:01:22.692288 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:01:25.703094 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:01:54.903429 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:00.791452 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:01.795084 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:02.794094 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:21.906065 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:50.954694 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:02:59.014819 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:03:05.062536 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:03:32.151389 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:03:44.173704 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:03:45.177432 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:04:05.214120 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:04:08.210476 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:04:10.226393 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:04:11.227394 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:04:26.244119 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:05:59.392168 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:06:28.452413 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:06:33.464734 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:06:42.464900 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:06:50.474834 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:06:52.491617 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:08.515236 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:12.522318 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:13.527026 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:18.530827 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:27.544274 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:34.555753 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:37.560309 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:44.574314 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:47.582699 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:07:53.593773 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:02.605545 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:04.608608 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:10.665933 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:22.692278 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:47.726528 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:50.732268 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:08:59.745430 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:02.047322 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:32988 -> 127.0.0.1:6379

10/28/2022-16:09:02.748507 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:03.751455 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:05.757076 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:16.817151 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:17.818293 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:19.822907 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:21.832301 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:23.848172 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:23.855228 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:34.151051 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:09:36.068216 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:09:37.870559 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:51.159853 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:09:52.130009 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:09:53.899059 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:53.906378 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:54.066696 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:09:56.909458 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:09:57.907306 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:09.219984 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:10:10.212603 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:10:10.922008 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:10.926212 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:11.931494 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:12.022373 [\*\*] [1:2221010:1] SURICATA HTTP unable to match response to request [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.28.53:5601 -> 192.168.28.15:57182

10/28/2022-16:10:12.927313 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:17.941477 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:10:26.948146 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:11:48.031425 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:11:48.031484 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:11:49.030385 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:11:56.050588 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:02.064410 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:04.066125 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:05.160775 [\*\*] [1:2101603:14] GPL WEB\_SERVER DELETE attempt [\*\*] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.28.15:57164 -> 192.168.28.53:5601

10/28/2022-16:12:18.099016 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:21.110661 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:27.119409 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:34.120105 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:42.130731 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:51.143051 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:12:54.154466 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:14.182582 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:19.179109 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:22.184023 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:36.212384 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:37.219746 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:13:48.226433 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:21.298194 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:30.312188 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:33.318571 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:42.329644 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:42.330388 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:48.345046 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:49.348314 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:14:54.353130 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:15:22.376773 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:15:42.397813 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:15:48.402404 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164

10/28/2022-16:15:53.412228 [\*\*] [1:2210044:2] SURICATA STREAM Packet with invalid timestamp [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 127.0.0.1:9200 -> 127.0.0.1:53164