Speaker: Barry Weymes, Security Engineer, Aramco Overseas Company

The Ever Increasing Need to Monitor SMB Traffic

A few years ago, SMB was not very widely known as an attack vector but that has progressively changing. This obscure and relatively unknown network protocol has gotten plenty of attention now and Bro protocol dissection has helped tremendously with that. As a Snort detection developer, it became recognizable that there was a serious gap in the detection capabilities with a traditional IDS generating alerts on this type of traffic. The context was missing: who/what/where. It is very difficult for security analysts to be fluent in how SMB works as it is immensely complex protocol and it's not easy to know what to look out for. The data Bro provides is essential in alert triage to give context to the alerts. In this presentation, I'd like to share some war stories about SMB traffic detection in corporate environments. I will demonstrate how SMB is increasing used during (internal) attacks. As an advanced Snort user, I shall touch on the differences between Snort/Suricata and Bro in detecting SMB traffic and how they can complement each other's along with host-based logs.