Detecting network and port scanning

Applicability

- Product: Splunk Enterprise or Splunk Cloud
- Feature: Search
- Function: Firewall log monitoring

To optimize the search shown below, you should specify an index.

Problem

Attackers scan networks for IP addresses and ports so they can find a good entry point into your organization. You want to see if scanning activity is coming from someone other than an authorized person internally.
Solution

Media, iframe, embed and object tags are not supported inside of a PDF.

Additional resources

For more great content from the Splunk Education and Training team, check out Splunk How-To on YouTube or sign up for a course. In addition, these Splunk resources might help you understand and implement this search:

- Data Descriptor: Firewall data