Detecting UDP service amplification abuse

Scenario: Your organization uses memcached to virtually pool memory and speed up dynamic web applications. While this is helpful for end users, as a security analyst, you know that its lack of authentication and authorization leaves your organization at risk for UDP service amplification abuse, a strategy often used in Denial of Service (DoS) attacks. You want to set up searches to monitor for indications of this type of attack. You can use Splunk software to find attack commands and examine bytes in flow records to detect amplification.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Splunk Stream
- Data: Network protocol data

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor for amplification abuse. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Communication over unsecured UDP
- Packet size disparities between source and destination
- Packet count disparities between source and destination

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Disabling UDP support if it is not required
- Setting up firewalls on your memcached servers

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Potential attacks detected: The number of packet size or packet count disparities between source and...
destination detected on your network

Additional resources

These additional Splunk resources might help you understand and implement this use case:

- Blog: Go with the flow: Network Telemetry (VPC data) in AWS
- Blog: Splunk Stream 7.2: Integration with Amazon VPC traffic mirroring
- Conf Talk: How to save money monitoring, managing, and securing your cloud using the Splunk App for AWS