JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service and Application Events

CYBER INCIDENT RESPONSE

Service/Application Events

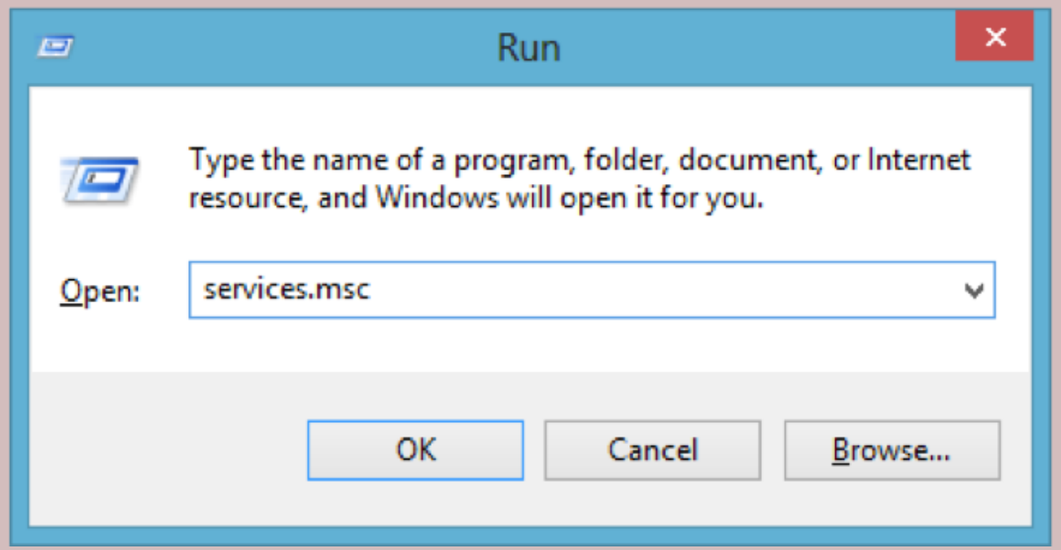
- Services and Applications should be monitored per good ITSM processes
  - Are they up/down?
  - Are they responding properly?
  - Are they functioning properly?
  - Are they conducting transactions properly?
  - Are they logging properly?

Service Anomalies

- Non-security issues:
  - Authentication errors
  - Permission issues
  - Services don't start on boot up
  - Service failures
- Investigate the issue to ensure it is not security related
- Use antivirus, antimalware, file integrity checking, and whitelisting to verify

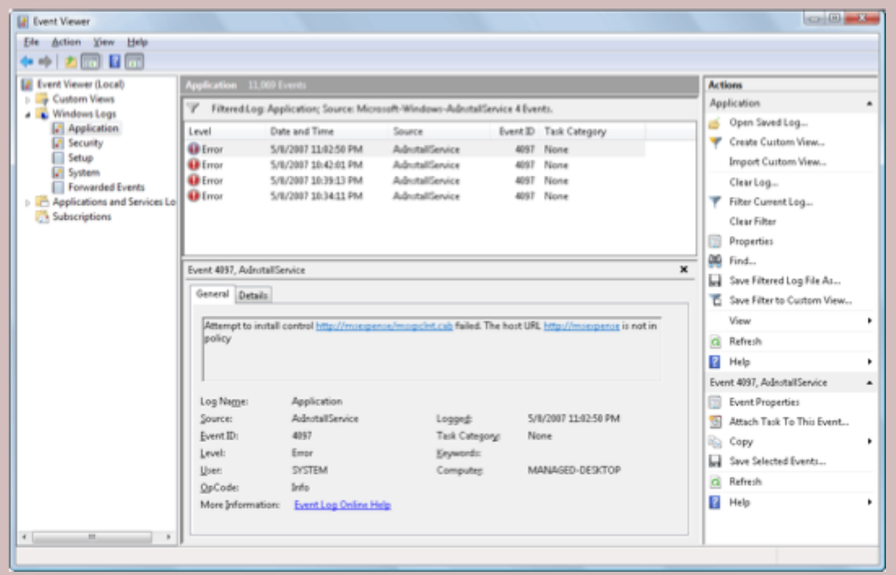
Checking Service Status

- Windows:
  - services.msc (GUI) or sc (command line)
- Linux:
  - service –status-all (command line)



Service/Application Logs

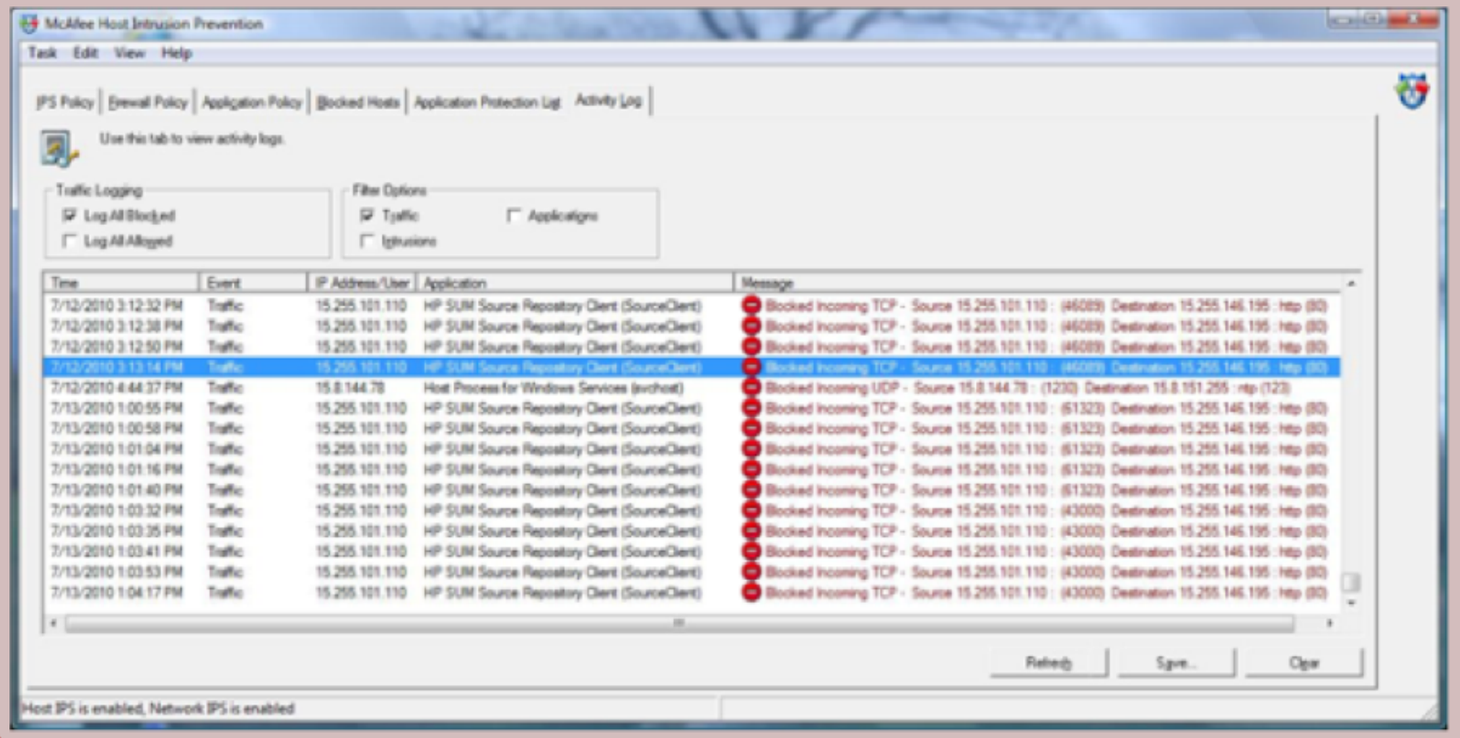
- Windows:
  - Use Windows Event Viewer to view Application Logs
- Linux:
  - Log to the /var/log directory
  - Use tail to view the end of the log files



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service/Application Behavior

- Create and understand a baseline
- Log/alert on anything outside of baseline



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service/Application Attacks

- Anomalous Activity
  - Doesn't match the typical behavior
  - Investigate the activity and solve
- New Accounts
  - Were they authorized?
  - Do they have excessive permissions?
- Unexpected Output
  - Improper output or garbage output
  - User and admin training imperative to determining the root cause

Service/Application Attacks

- Unexpected outbound communication
  - Why is the application sending out data?
  - Detect with network monitoring
- Service Interruption
  - Simple issue or a DDoS?
  - Monitoring tools can help determine reason
- Memory Overflows
  - Causes OS errors and crashes
  - Monitoring for them is hard
  - Detecting after a crash is easier

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE