

# Cat Scan II Big Dog

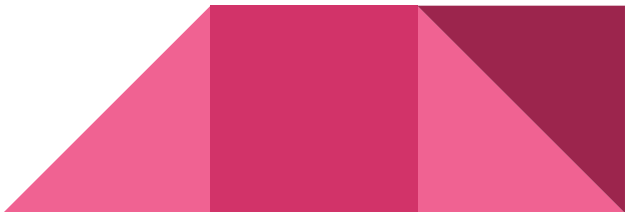
By Derek Mayen

# Executive Summary

The company *Big Dog* has asked us to assess the risks and vulnerabilities that their assets are exposed to, as well as propose any mitigation methods and sensors to help protect their valued assets. The assets that were presented to us were as follows listed from most important to least:

- Privacy (P)
- Proprietary (IP)
- Financial(F)
- Financial/Accounting(F)
- Security Management(SM)
- Systems(S)

## Sensors Recommended

- EXE/Script Sensor
  - HTTP Advanced Sensor
  - SSH Script Sensor
  - Windows Update Status (Powershell) Sensor
  - HTTP Advanced Sensor
- 

# Overview of the Process

- Operating System Scan
- CVE Research (Common Vulnerabilities and Exposures)
- CVSS Calculations (Common Vulnerability Scoring System)
- Sensors & Mitigations



# Vulnerabilities

## **Windows Systems**

- Scripting Engine Memory Corruption
- Windows Storage Services Elevation of Privilege

## **Linux**

- Integer-Overflow

## **Windows Server**

- Windows Security Feature Bypassing



# Table of Devices

Devices	Sensors	Thresholds	SIL's	IoC's
Windows 1&2	EXE/Script Sensor	N/A	Level 3	Incorrect Value of memory stability
Windows 1&2	HTTP Advanced Sensor	2(warning) 3(error)	Level 3	Too many failed authentication attempts
Linux	SSH Script Sensor	80% of disk space used up (warning) 90% of disk space used up (error)	Level 3	Unusual disk space usage
WinServer	Windows Update Status (Powershell) Sensor	N/A	Level 3	Latest Updates Not Being added
Kali	HTTP Advanced Sensor	2(warning) 3(error)	Level 3	Too Many failed authentication attempts

# Recommendations

Some Industry Best Practices include:

- Principle of Least Privilege
- MFA (Multi-factor authentication)
- Isolating potentially malicious or untrusted code or processes
- Data Execution Prevention

