Helping You Piece IT Together

Best Practices for Log Monitoring

http://www.bhconsulting.ie info@bhconsulting.ie

Introduction

- What are logs?
- Why are logs important?
- The Challenges
- Recommended Best Practises
- Further Reading

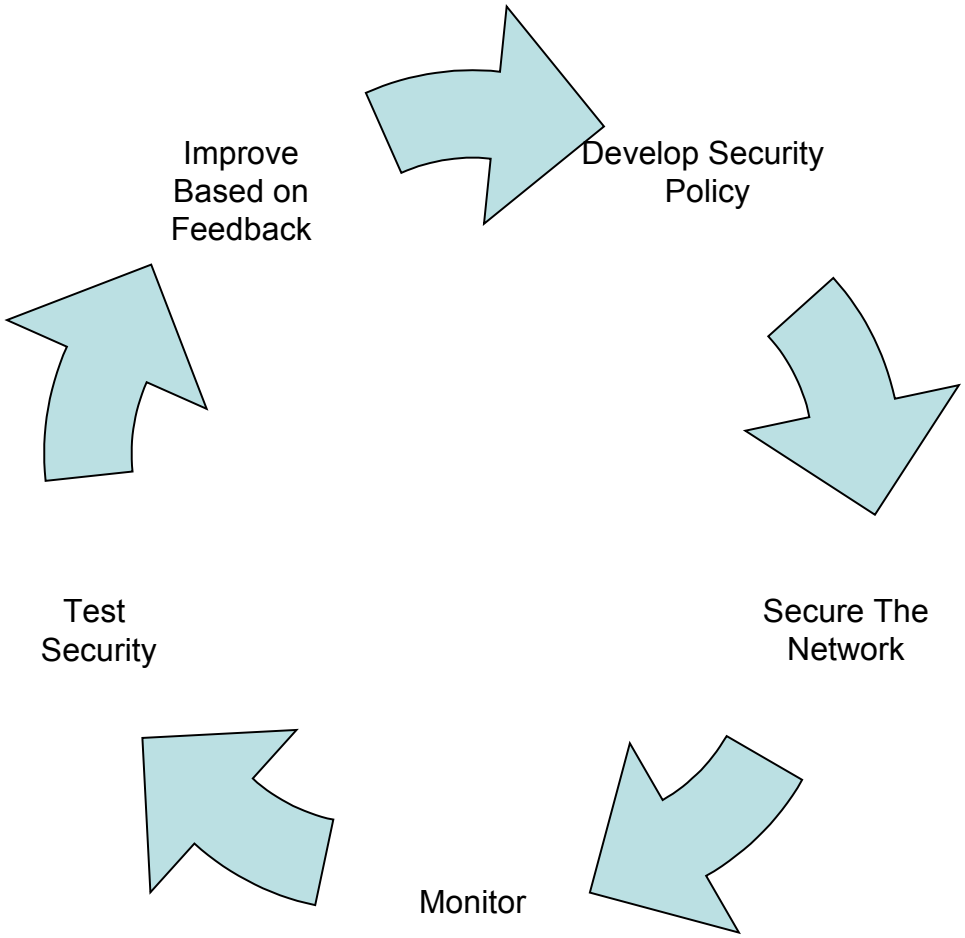
What Are Logs?

- Historical Record of events that happened.
- Records events and status of systems in a time sequential format.
- Record of activity on the system/network.
- Provide an Audit trail of who done what, where, when and why (5 Ws)

Why are Logs Important?

- **Logs can assist us in;**
  - Determining what happened - Audit Trail
  - Intrusion Detection
  - Incident Containment
  - Forensic Analysis
  - Proactive Protection
  - Real Time Alerts
  - Providing a Network Baseline
  - Determining the Health of the Network
    - Troubleshooting issues
    - Proactive maintenance

Monitoring as Part of Security Process

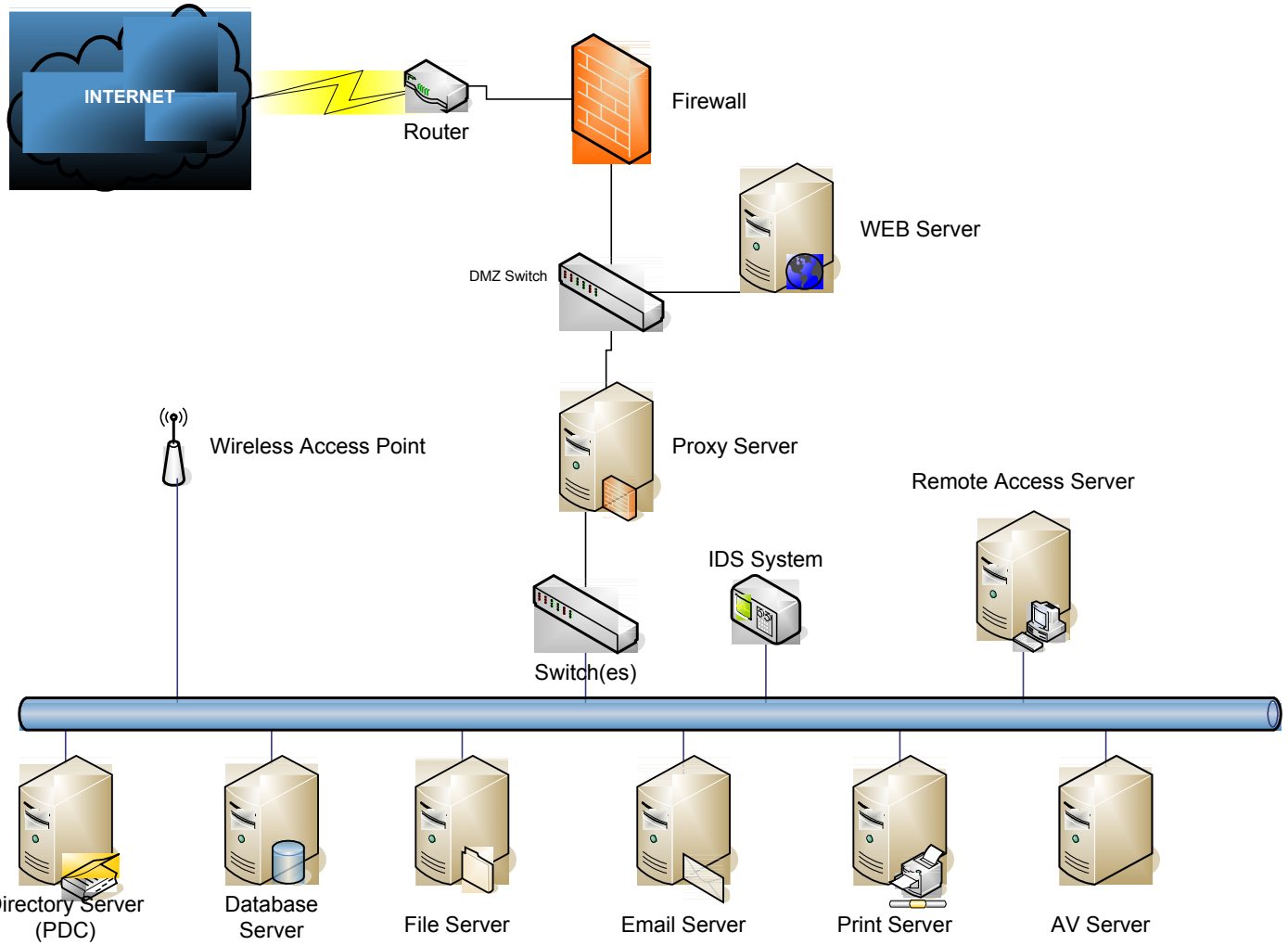


Why are Logs Important?

- **Logs are everywhere;**
  - Operating Systems
  - Applications
  - Device logs
    - Routers
    - Firewalls
    - IDS
    - Switches

- **All this information should be making our jobs easier. Right?**

Typical Network



The Challenges

- **Different vendors different log formats.**
- **Regulatory Requirements.**
- **Logs were written by developers**
  - Format is not easy to read
  - Messages can be obscure
- **Logs contain enormous amount of information.**
- **Identifying anomalies can be difficult**
  - Probes over time

The Challenges

- **Managing Logs can be Expensive;**
  - Log analysis is a unique skill.
  - Looking at all events takes time.
  - Logs can consume a lot of disk space.
- **Volume of information is huge**
- **No one size fits all.**
  - Each network is unique

Too Much Information !!!

Best Practices

- **Develop logging Policy**
- **Determine what information is relevant to you.**
  - What devices are important?
  - What events are important?
  - Don't forget to turn on logging!
  - Timing of events, e.g. user logons in morning.
  - What reports you and the business want/need?
  - Group servers into zones based on their function or criticality and prioritise events accordingly.
- **Baseline your systems & network.**
  - Determine how your network normally behaves.
  - Repeat at regular intervals
- **Secure log files on all devices.**
  - Encrypt logs
- **Ensure all devices use same time source.**
  - If using more than one time zone use UTC.
  - Use NTP protocol from a secure source to synchronise time.

Best Practices

- **Centralise log collection**
  - Dedicated server to collect all logs.
    - Be careful of network traffic volumes.
    - Be aware of limitations of server to process number of events.
  - Configure all devices send logs to central log server.
  - Make sure central server is secure.
  - Secure transmission of logs.
    - e.g. Syslog uses UDP by default. Consider using IPSec or next generation Syslog (Syslog-NG)

Best Practices

- **Normalise the data**
  - All events such as Windows, Syslog, SNMP etc. should be normalised into same format.

- **Review the Logs**
  - Ensure logs are regularly reviewed
    - Manually
    - Automatically
      - Scripts
      - Commercial Tools
      - Freeware Tools

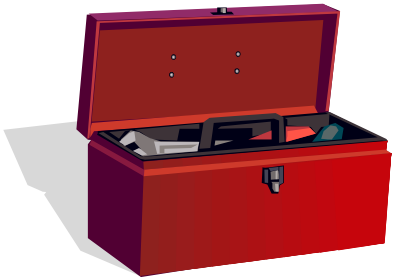
Best Practices

- **Log Rotation**
  - Determine time schedule
    - Based on volume of data
  - Develop meaningful naming convention.
  - Move data to rotated file
- **Log Retention**
  - Based on disk space.
  - May be regulatory requirements.
  - Archive onto WORM type devices and store in secure area.

Important Windows Events

- **Local Logon Attempt Failures**
  - Event IDs 529, 530, 531, 532, 533, 534 & 537.
- **Domain Logon Account Failures**
  - Event IDs 675, 677
- **Account Misuse**
  - Event IDs 530, 531, 532, 533
- **Account lockout**
  - Event ID 539
- **Terminal Services**
  - Event IDs 682, 683
- **Creation of a User Account**
  - Event IDs 624, 626
- **User Account password Change**
  - Event IDs 627, 628
- **User Account Status Change**
  - Event IDs 626, 629, 630
- **Modification of Security Groups**
  - Event IDs 632, 633, 636, 637
- **Modification of Security Log**
  - Event IDs 612, 517
- **Policy Change**
  - Event IDs 608, 609
- **Process Tracking**
  - Event IDs 592, 593 (note due to volume of log entries only monitor process tracking during an investigation.)

Tools



- **Convert Windows Events to Syslog**
  - WinSyslog http://winsyslog.com/en/
  - EventReporter http://www.eventreporter.com/en/
- **Commercial Monitoring tools**
  - GFI LANguard (Windows Only) - http://www.gfi.com/lanselm/
  - Symantec - http://www.symantec.com
  - HP Openview - http://www.managementsoftware.hp.com/products/a-z.html
  - IBM Tivoli - http://www-306.ibm.com/software/tivoli/
  - CA Unicentre - http://www3.ca.com/solutions/product.asp?id=2869
  - Intellitactics Security Manager - http://www.intellitactics.com/blue.asp?PageID=26
  - Netforensics - http://www.netforensics.com/
  - ArchSight - http://www.arcsight.com/
- **Open Source**
  - Nagios (Open Source) - http://www.nagios.org/

Links

- **Log Analysis website - Tina Bird & Marcus Ranum**
  - http://loganalysis.org/
- **Counterpane's website**
  - http://www.counterpane.com/literature.html
- **CERT Coordination Centre**
  - Establish a policy and procedures that prepare your organization to detect signs of intrusion
    - http://www.cert.org/security-improvement/practices/p090.html
  - Detecting signs of suspicious behavior
    - http://www.cert.org/security-improvement/practices/p091.html
    - http://www.cert.org/security-improvement/practices/p092.html
  - Monitor for unexpected behavior
    - http://www.cert.org/security-improvement/practices/p095.html
- **The SANS reading room**
  - http://www.sans.org/rr/whitepapers/logging/
- **Event ID website given explanations to MS events**
  - http://www.eventid.net/

Questions ?