Secure Implementation of Logging and Network Monitoring

Indian Computer Emergency Response Team
Department of Electronics & Information Technology
Ministry of Communications & Information Technology
New Delhi

Ruchi Gola,Scientist-C,
ruchi@cert-in.org.in

Agenda

- Logs & Monitoring
- Monitoring Logs for Security
- Monitoring logs for understanding the systems
- Challenges in Log Management
- Solution to this challenge
- System Information and event management (SIEM) technology
- Benefits of SIEM tools solves these issues
- A comparative situation with example of the attack taxonomy
- A comparative situation with example of the attack taxonomy……with SIEM implemented
- Secure Implementation of Logging and Network Monitoring-Best Practices compliance
- References

Logs & Monitoring

- What are logs?
  - Provide an audit trail of who done what, where,when and why(5 Ws)

- Why monitor your logs?

  - Security
    - Proactive
    - Reactive
  - Understand your systems
    - Good system administration
    - Identify configuration errors

Monitoring Logs for Security

- Proactive - identify a pattern before it becomes serious

- Reactive - understand what happened
  - Incident handling
  - Viewing troubleshooting messages
  - Watch for network events such as attacks, real-time alerts and service denials.

Example of proactive monitoring ofLogs for Security

/var/log/auth.log
Sep 2 07:43:21 sshd[24760]: refused connect from 220-128-206-131.HINET-IP.hinet.net (::ffff:213.149.206.131)
Sep 2 07:44:23 sshd[24765]: refused connect from 220-128-206-131.HINET-IP.hinet.net (::ffff:213.149.206.131)
Sep 2 07:46:41 sshd[24770]: refused connect from 220-128-206-131.HINET-IP.hinet.net (::ffff:213.149.206.131)
Sep 2 07:50:14 sshd[24779]: refused connect from 220-128-206-131.HINET-IP.hinet.net (::ffff:213.149.206.131)

Example of reactive monitoring of Logs for Security

Incident Handling:

- Review Logs as they are invaluable in detecting and tracking attempted intrusions and other suspicious activity.

- Eg. 2008-04-15 01:41:42 **202.x.y.4** - W3SVC12 MURWSH002 **202.m.n.o** 80 GET /images/down_banner2.gif - 200 0 58403 690 2093 HTTP/1.1 www.anywebsite.gov.in Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.8.1.13)+Gecko/20080311+Firefox/2.0.0.13 - http://www.anywebsite.gov.in/content/agenda/default.asp?comid=8;UPDATE%20committees%20set%20CommitteeName=**0x4f3C68313E776E65642062792046617354206F662053474346E69635F5330756C732056657269 6E20656820756D61206269626F6E612061686569 6F6169686F613C2F68313E**%20FROM%20committees.

- In the above log entry, the c-ip 202.x.y.4 has successfully inserted the hexadecimal code string in CommitteeName column of the table committees.The ASCII equivalent of the hexadecimal code string '**0x4f3C68313E776E65642062792046617354206F662053474346E69635F5330756C732056657269 6E20656820756D61206269626F6E612061686569 6F6169686F613C2F68313E**' is '**?O<h1>wned by FasT of S4t4nic_S0uls Verin eh uma bibona aheioaihoa</h1>**

Monitoring logs for understanding the systems

Good system administration

- An important part of a system administrator's job is to regularly check various log files.

- Identify configuration errors

  Eg. 1) /var/log/kern.log – Contains information logged by the kernel. Helpful for administrator to troubleshoot a custom-built kernel.

  2) /var/log/setroubleshoot/ – SELinux uses setroubleshootd (SE Trouble Shoot Daemon) to notify about issues in the security context of files, and logs those information in this log file.

Challenges in Log Management

- Logs are generated at different devices of different vendors who offer different log formats :
  - operating systems,
  - applications
  - device logs
    - router
    - firewall
    - switch
    - IDS & IPS

The logs of all these devices makes up correlation possible behind a security breach incident in the organisation

- Regulatory Requirements.
- Logs were written by developers ,therefore format is not easy to read ,messages can be obscure

Challenges in Log Management

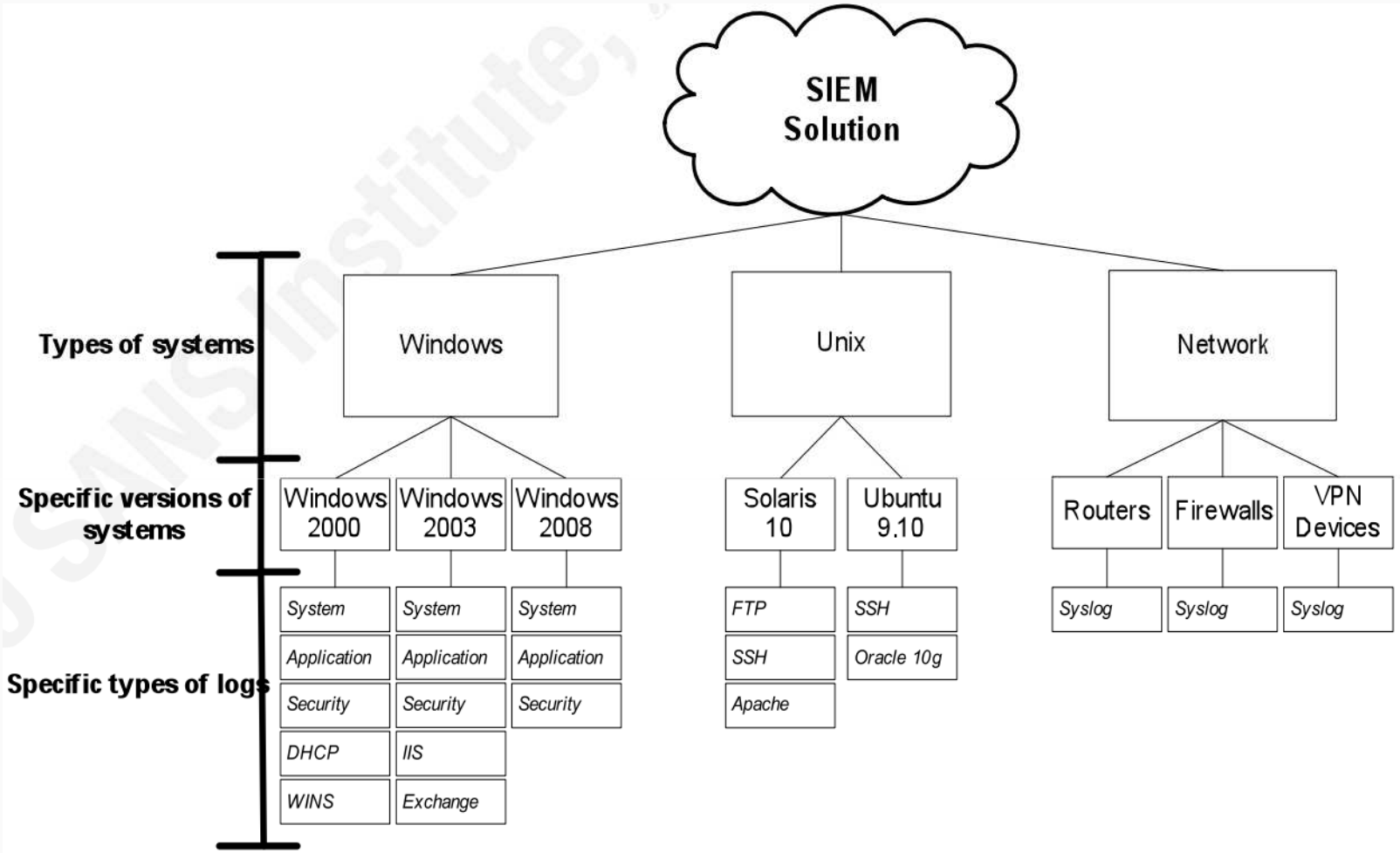
- Logs contain enormous amount of information.
- Identifying anomalies can be difficult
- **Managing Logs can be Expensive;**

  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 as each network is unique**

- Regular backups of all log files to be conducted at scheduled intervals
- Log files can easily become tremendous in size if set to monitor every detail. Sometimes, this is considered a burden;
- The organization's secure disposal policies should be used when wiping and shredding log data and media.

Solution to this challenge



Reference: http://www.sans.org/reading_room/whitepapers/auditing/effective-case-modeling-security-information-event-management_33319

System Information and event management (SIEM) technology

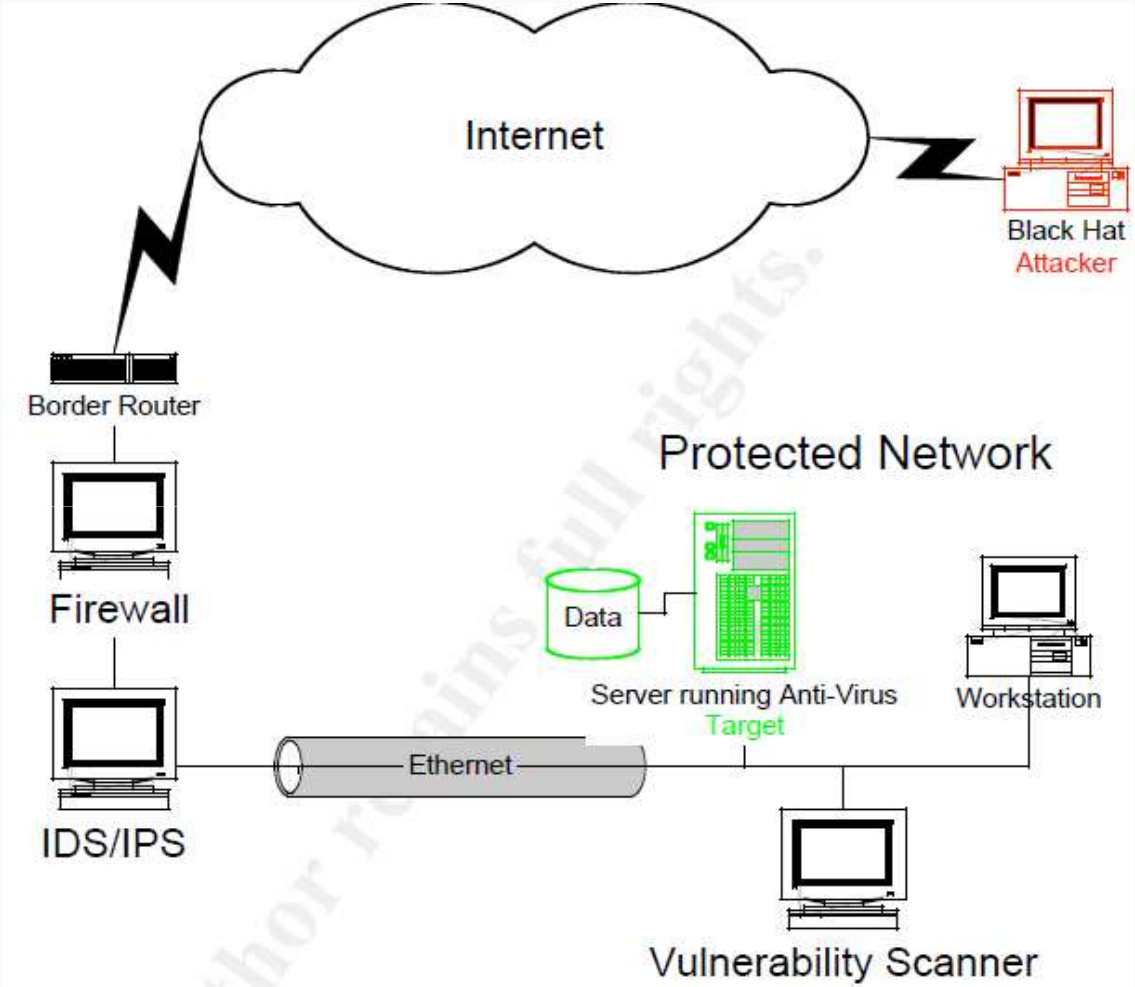
- Centralized Syslog Server :

This facilitates **record-keeping** of all systems and network activity at a single locations, which offers advantages such as,

- it can be placed at different segments for secure storage,
- allows better co-relation of attacks across different platforms,
- easier backup policies,
- real-time alert generation using tools like Swatch(simple watcher)
- security benefit that at least with a central syslog server the entries associated with the attack itself can be obtained even if the original machine has got hacked and the traces being wiped off by intruder.

Benefits of SIEM tools solves these issues

A comparative situation with example of the attack taxonomy



Basic Network diagram with *Single Firewall, IPS, and Vulnerability Scanner*

1. **Attacker Scans the Firewall** (using NMAP,Firewalker, HPING, etc…) to determine the responding IP addresses, open ports on it.Conducts this phase in Low and Slow manner to avoid triggering automatic Protections

2. **Finger Printing**
Continued, targeted scan (using NMAP, HPING, etc…)again to determine the operating system and applications running on discovered hosts.

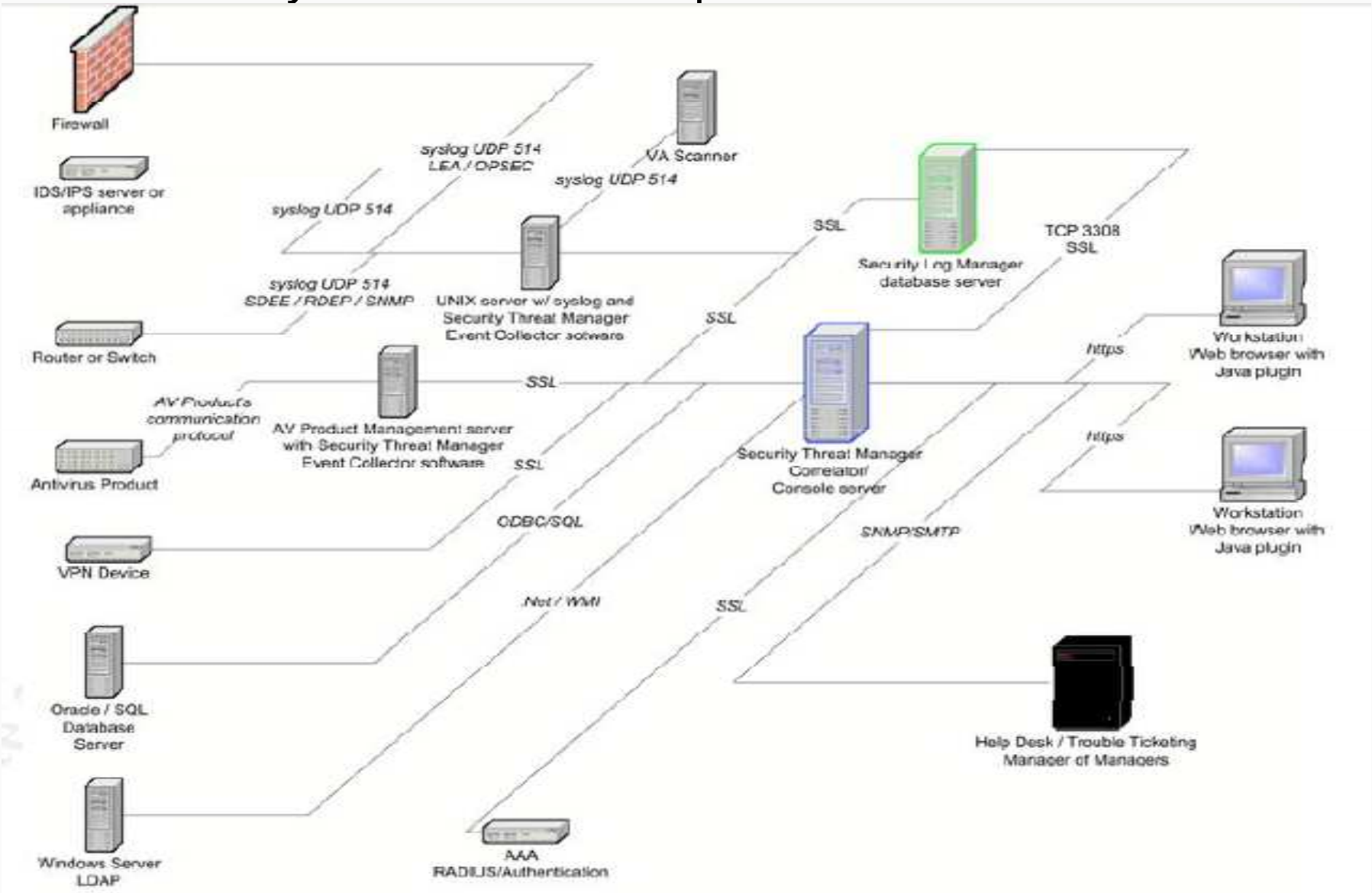
3. **Targeting with IDS Evasion**
Send targeted attacks of known vulnerabilities(buffer overflows, With Fragmented packets) with signature evading patterns (metaslpoit)

A comparative situation with example of the attack taxonomy…….contd.

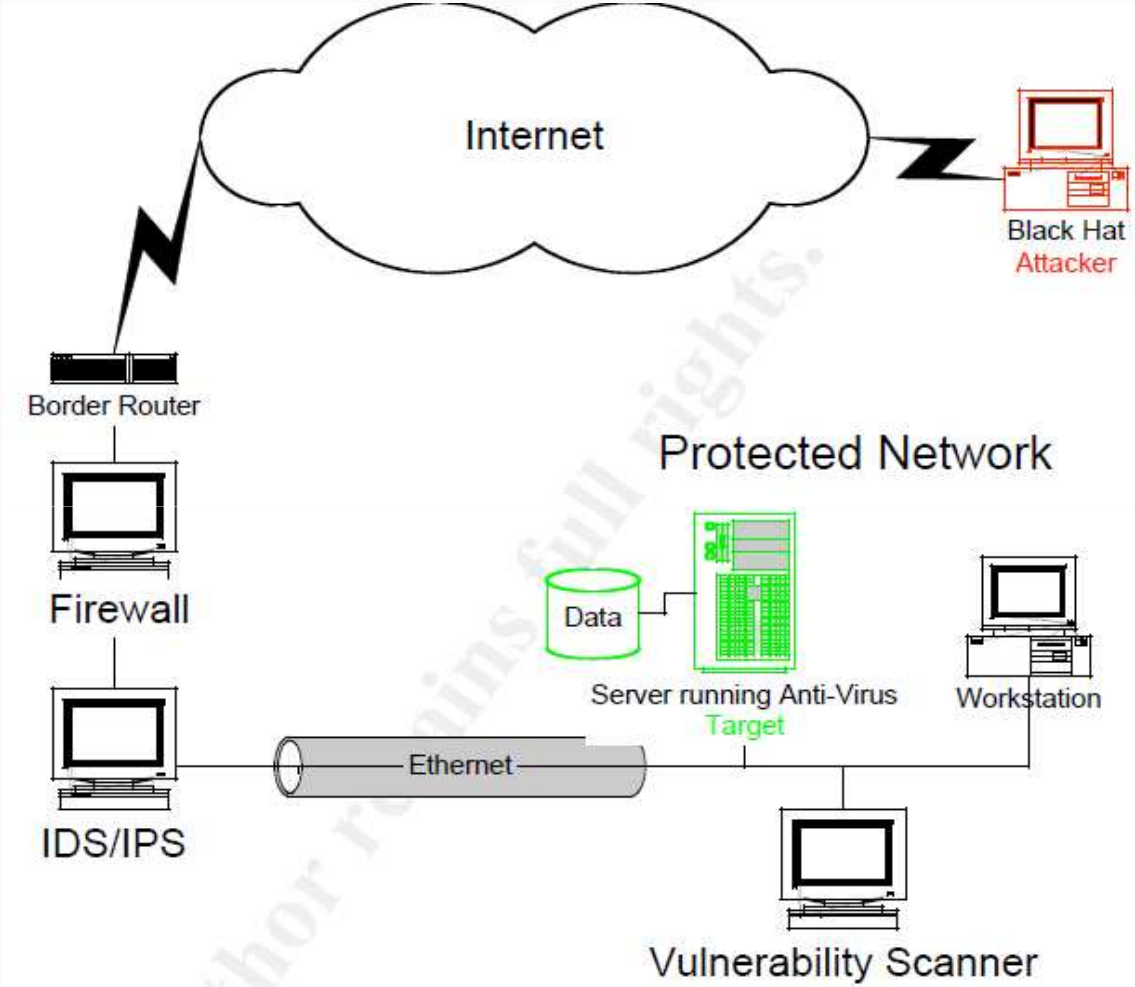
4. **Compromise** System Crash, Denial of Service, or Data theft Install sniffers, backdoors or rootkits for ongoing access DSNIFF. Ettercap, Ethereal ,Netcat, VNC,BackOrifice, LRK, AFK, KIS

In each phase ,the attacker has crafted the attack phase such as to bypass a single individual protection device, having learned how to penetrate the preceding device.

A comparative situation with example of the attack taxonomy……with SIEM implemented



A comparative situation with example of the attack taxonomy……with SIEM implemented….contd.



Basic Network diagram with *Single Firewall, IPS, and Vulnerability Scanner*

1. **Attacker Scans the Firewall** The Router or Firewall sends events to SIEM indicating port scans and an alert is built at minor/warning level.

2. **Finger Printing**
The IDS/IPS reports system scans, and other possible signature matches, and the alert is raised to an elevated level.Security staff is notified (email, pager,etc...).

3. **Targeting with IDS Evasion**
The firewall reports fragmented packets, the IDS may report certain signatures, and the alert level is raised to high.If the IDS sees an event and the vulnerability scanner knows the event can compromise a system, the alert is escalated to critical.Security staff is notified of a high probability threat and automated responses are taken.

Secure Implementation of Logging and Network Monitoring-Best Practices compliance

- **Develop logging Policy**
- **Determine what information is relevant to the oraganisation.**

  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(GMT).

  Use NTP protocol from a secure source to synchronise time.

Secure Implementation of Logging and Network Monitoring-Best Practices compliance

- **Centralise log collection**

  Dedicated server to collect all logs.

  Be aware of network traffic volumes.

  Be careful of limitations of server to process number of events.

  Configure all devices send logs to central log server.

  Make sure central server itself is also secure. Secure transmission of logs.

  e.g. Syslog uses UDP by default. Consider using IPSec or next generation Syslog (Syslog-NG)

- **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.

Secure Implementation of Logging and Network Monitoring-Best Practices compliance……contd.

- 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

References

- **Log Analysis website(http://loganalysis.org/)**
- **The SANS reading room (h**ttp://www.sans.org/rr/whitepapers/logging/)
- **Event ID website given explanations to MS events h**ttp://www.eventid.net/
- **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/
- **Guidelines for Auditing and Logging at CERT-In website**
- **A Practical Application of SIM/SEM/SIEM Automating Threat identification**(www.sans.org)

Thank you