

Network Forensics



Omveer Singh

Additional Director / Scientist 'E'

omveer@cert-in.org.in

November 28, 2009

Indian Computer Emergency Response Team (CERT-In)

Department of Information Technology

Ministry of Communications & Information Technology

Government of India

New Delhi

Agenda

- Network Forensics
- Network Forensics Analysis Tools (NFAT)
- N/w Traffic Capturing
- N/w Traffic Analysis
- Internet Forensics
- Email Forensics
- Log Files Analysis
- References

Cyber Forensics

- The art of gathering evidence during or after a crime
 - Reconstructing the criminal's actions
 - Providing evidence for prosecution
- Forensics for computer networks is ***extremely*** difficult and depends completely on the quality of information you maintain

Cyber Forensics

- **Computer Forensics**
- **Mobile Forensics**

Subcategories of Computer Forensic Analysis

- **Storage Media Analysis**
 - Examining storage media for evidence
- **Source Code Analysis**
 - Software Source Code Examination for malicious signatures
- **Network Analysis**
 - **Scrutinize network traffic and logs to identify and locate the suspicious system**

Network Forensics

What is Network Forensics?

- Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other security incidents.

Network Forensics

- Scrutinising network traffic and logs to identify and locate the suspicious system
- Network forensics is the process of examining network traffic
 - After-the-fact analysis of transaction logs
 - Real-time analysis via network monitoring
 - Sniffers
 - Real-time tracing

Network Forensics

- Sniffers
- Clear http
- Encrypted http
- Login id & password recovery
- Capturing incoming / outgoing e-mails' text

Network Forensics Analysis Tools (NFAT)

- NFATs must do the following:
 - Capture network traffic
 - Analyze network traffic according to user needs
 - Allow system users to discover useful and interesting things about the analysed traffic

NFAT Tasks

- Traffic Capture
 - What is the policy?
 - What is the traffic of interest?
 - Internal/External?
 - Collect packets: tcpdump
- Traffic Analysis
 - Sessionising captured traffic (organise)
 - Protocol parsing and analysis
 - Check for strings, use expert systems for analysis
- Interacting with NFAT
 - Appropriate user interfaces, reports, examine large quantities of information and make it manageable

NFAT v/s IDS, Firewall

- IDS attempts to detect the activity that violates an organization's security policy by implementing a set of rules describing preconfigured patterns of interest
- Firewall allows or disallows traffic to or from specific networks, machine addresses and port numbers
- NFAT synergizes with IDSs and Firewalls :
 - Preserves long term record of network traffic
 - Allows quick analysis of trouble spots identified by IDSs and Firewalls

Network based IDS (NIDS)

- Detect malicious activity by monitoring network traffic – DoS attacks, port scans, attempts to crack into computers
- Collect data from the network or a hub / switch to
 - Reassemble packets
 - Look at headers
- Try to determine what is happening from the contents of the network traffic
 - User identities, etc inferred from actions

Honeypots

- Network Forensics and Honeypot systems have the same features of collecting information about computer misuses
- Honeypot system can lure attackers and gain information about new types of intrusions
- Network forensics systems analyze and reconstruct the attack behaviors
- These two systems integrated together build a active self-learning and response system to profile the intrusion behavior features and investigate the original source of the attack.

N/w Traffic Capturing Systems - 1

- “***Catch-it-as-you-can***” systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.

N/w Traffic Capturing Systems - 2

- **“Stop, look and listen”** systems, in which each packet is analysed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

N/w Traffic Analysis

- Tcpcmdump + *strings*
- Iris Network Traffic Analyser
 - Session reconstruction
 - Data capturing
 - Network performance analysis
- Wireshark

Analysing Network Traffic

- By understanding the structure of the protocol headers at each layer, and the meaning of the values carried in the header fields, it is possible to understand the behaviour of the network traffic

Analysing N/w Traffic : Using a Protocol Analyser

- Data making up a frame is sent as a series of bits. It is the protocols that allow various processes to differentiate between different fields and components in this bit stream.
 - For example; the IP protocol defines the field for the destination IP address so that the process can extract this information and use it to forward the packet. It also identifies where the data it is carrying (the TCP segment in this case) begins.
- When packets (or frames) are captured using packet capture software such as **Wireshark**, the bit stream making up that frame is displayed as a string of hexadecimal digits (showing this in binary would make it too unmanageable)

N/w Traffic Analysis (contd..)

- 'strings' to find text from traffic stream
- 'grep' to find specific words or phrases in the recovered strings
- get – network's web traffic
- quit – FTP control session / POP3 session / NNTP session
- privmsg – IRC (internet relay chat) session
- TCP connection on port 23 with telnet commands – telnet session
- TCP connection on port 23 with string 'YMSG' – yahoo messenger session

N/w Traffic Analysis will provide

- Contents of people's emails
- User ids & passwords (if plaintext, FTP, POP3)
- Determine web pages viewed
- Contents of a person's shopping cart

Analysis

- Examine log files
- Look for sniffers
- Look for remote control programs (netbus, backorifice, etc)
- Look for possible hacker file sharing or communications programs (eggdrop, irc, etc)

Analysis (contd..)

- Look for privileged programs
find / -perm -4000 -print
- Look for file system tampering
(use tripwire or backups)
- Examine 'cron' and 'at' jobs
- Look for unauthorized services
netstat -a
check inetd.conf

Analysis (contd..)

- Look for password file changes or new users
- Check system and network configurations
 - Pay close attention to filtering rules
- Look for unusual files
 - Depending on the size of your disks:
`find / -print | more`
- Look at all your hosts, especially servers

Backtracking

- Nowadays hackers are increasingly sophisticated about hiding tracks
 - The ones that are good, you won't catch
 - The ones that you can catch aren't worth catching
- Very few good tools for backtracking are available

Hidden Directories

- Search folders/directories for pirated s/w; may be hidden
- Pirates s/w are often hidden in FTP or web areas using weird directory names:
 - “...”
 - “ ” (space)
 - “normal ” (normal with space after it)
- Check FTP areas for new directories

Finding Hacker-Prints

- Search suspected infected system for new files:
 - find / -mtime -30 -print
 - Use tripwire
 - Restore filesystems to a different disk and compare all the files (slow and painful!)

Internet Forensics

Some Popular Internet Browsers

- Internet Explorer
- Netscape Navigator
- Mozilla Firefox
- Google Chrome

Internet Access Analysis

- Network Access Logs
- Access Logs from ISP
- Websites visited, time & duration
- Use of proxy websites
- s/w tools / utilities available / installed in the user system

Internet Forensics

- Internet or Web forensics is the process of piecing the information together - where and when a user has been on the Internet.
- Temporary Internet Files
- History of websites visited
- Cookies
- User activity recreation

e-Mail Forensics

Email Forensics

- Email forensics is the study of source and content of electronic mail as evidence.
 - identifying the source system, location & actual sender
 - recipient of a message
 - date/time of sending email.
 - E-mail may be very incriminating too.
- e-Mail Headers
- deleted emails

Some e-Mail Boxes File Extensions

- MS Outlook .pst, .ost
- Outlook Express .dbx, .mbx
- AOL .idx
- Mac .eml
- Lotus Notes .nsf
- Netscape .snm, .msf
- MS Exchange .edb

Internet based e-Mail

- Gmail, Hotmail, Yahoo, etc.
- There is no local storage of emails
- For analysis, email server user access logs and user mailbox required
- Rest of the analysis is like Internet Access
Analysis and access logs from ISP are required

e-Mail Analysis

- Client System IP
- Message ID
- ESMTP ID
- e-Mail Server Access Logs
- Access Logs from ISP
- s/w tools / utilities available / installed in the user system

Spam



Spammer

Decides the contents of the spam and number of users to be targeted

From Doris Boyce <9ZvasrG@dsprelated.com>
 Sent Tuesday, June 26, 2007 12:12 pm
 To info@cert-in.org.in
 Subject caputo melanin accreditation ::

Hello,

Visit our new online store and save upto 85
<http://www.pharmstockrx.com/>

All popular ones are available with free shipping worldwide with no need for any visits.
<http://www.canadianrxstock.com/>

Dr. ?Carolyn Goss

Spoofer Emails

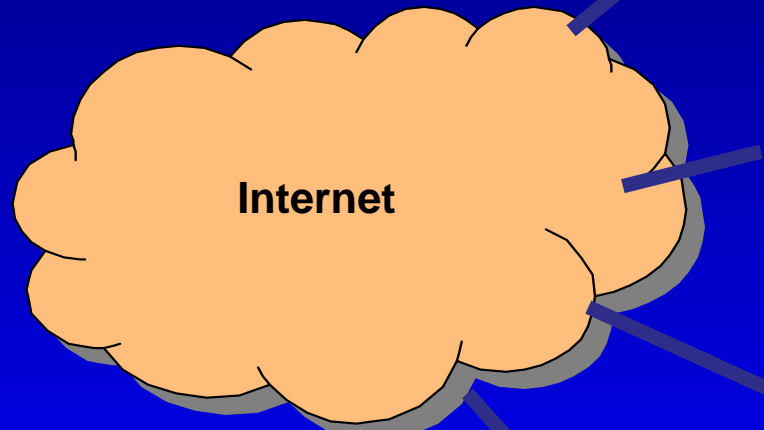
are sent using –

- Open relays
- Compromised systems
- Self owned email servers
- Temporary accounts
- Hijacked accounts

Spam



Spammer
Searches for carrier to launch
the campaign



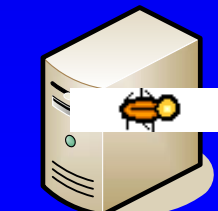
**Open Relay
Mail Server**



**Open Proxy
Server**



BOTs



**Mass Mailing
Worm**

Log Analysis

Log Files Analysis

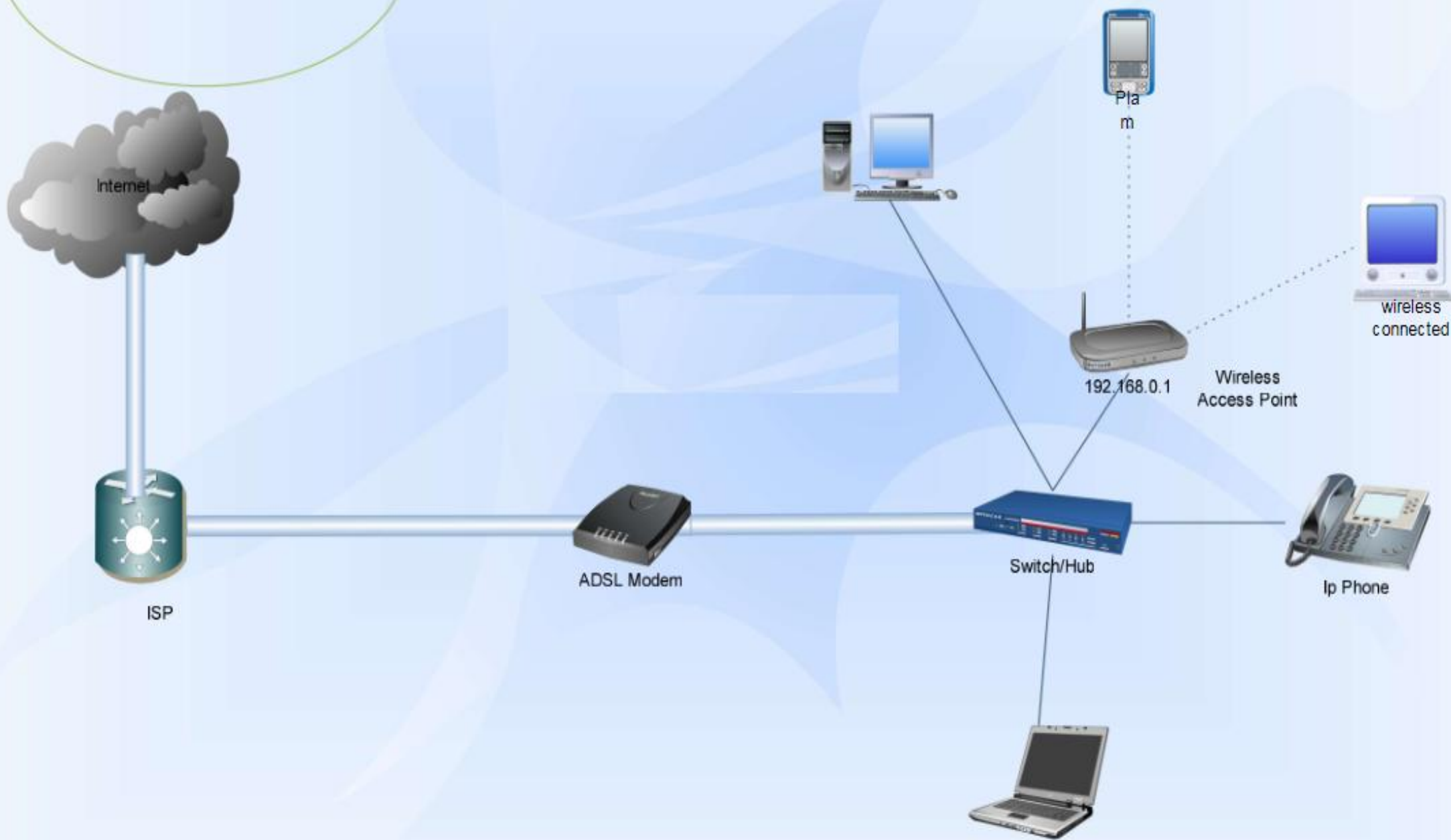
Essential to reconstruct the chain of events:

- Victim system's log files (Event Logs)
- Web Server (IIS / Apache Logs), Mail Server Logs
- IDS / IPS, Firewall, Router log files
- Log files of the system used for crime
- Access log details of the system used for crime
- from ISP
- SysLog Server Logs

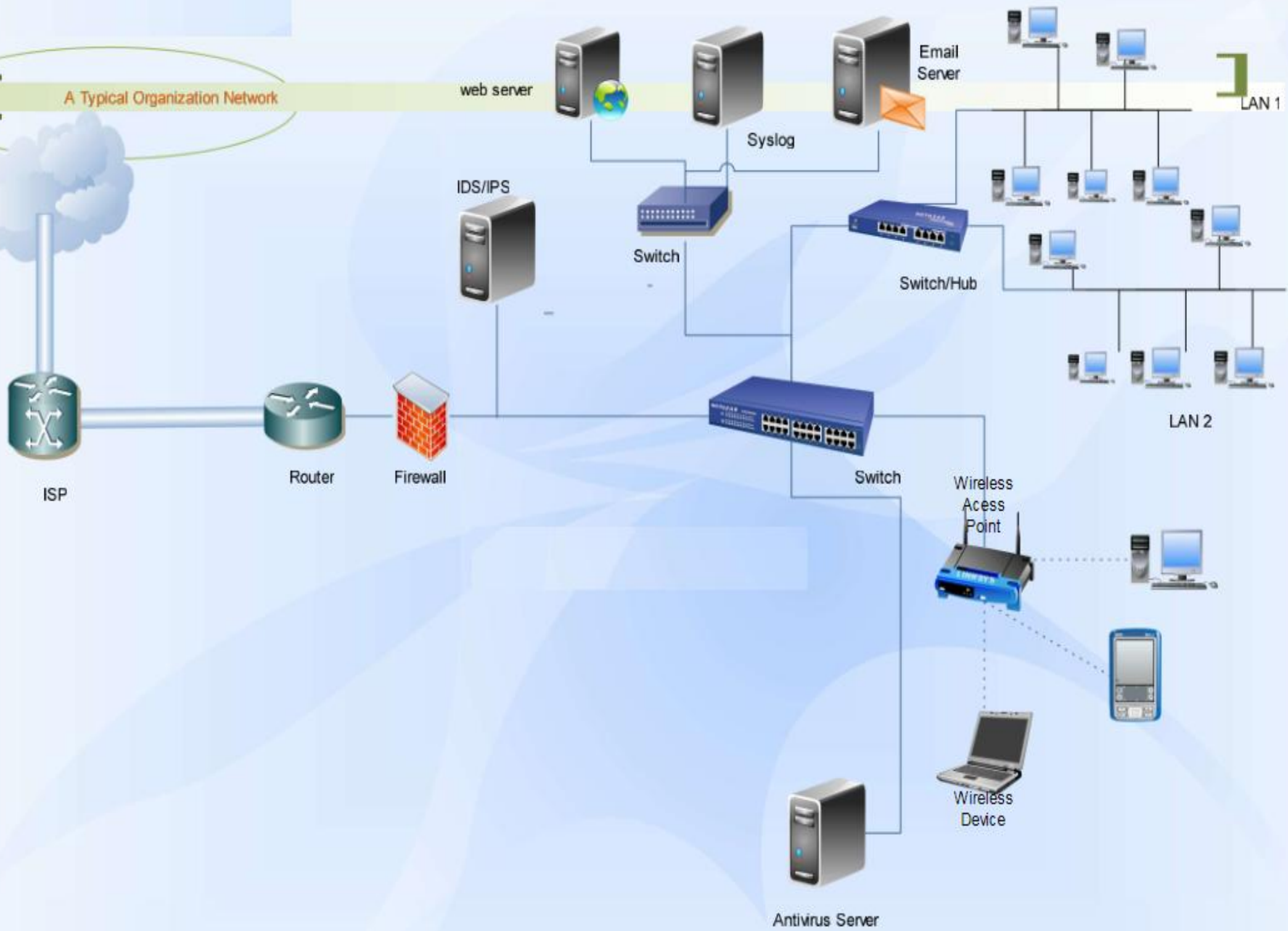
Handling of Log Files - as Evidence

- Must not be modifiable
 - Copy to a protected media (only once writable)
 - Bit-stream copy to Optical media
- Must be complete
 - All superuser access
 - Login and logout details
 - Attempts to use any controlled services
 - Attempts to access critical resources
 - E-mail details
- Appropriate retention

A Typical Home Network



A Typical Organization Network



web server

Email Server

LAN 1

Syslog

IDS/IPS

Switch

Switch/Hub

LAN 2

ISP

Router

Firewall

Switch

Wireless Access Point

Wireless Device

Antivirus Server

Log Files

- Windows Hosts – Event logs
- Linux Hosts – Syslog
- Web server - IIS logs
- Web server – Apache logs
- IDS / IPS logs

Log Files (contd..)

- Security Logs
 - Login logs
 - Remote entry logs
 - Real time monitoring logs
- System Logs
 - Authority logs
 - Accounting logs
 - Error logs

Log Files (contd..)

- Application Logs
 - Events reported by user applications
 - Internal application errors
 - ID of users using application
 - Entry & exit time of application use

Logs - Scanning incident

```

Nov 1 18:52:13 125.17.139.212:3056 -> 128.173.8.54:139 SYN *****S*
Nov 1 18:52:15 125.17.139.212:3041 -> 128.173.8.39:139 SYN *****S*
Nov 1 18:52:16 125.17.139.212:3051 -> 128.173.8.49:139 SYN *****S*
Nov 1 18:52:16 125.17.139.212:3053 -> 128.173.8.51:139 SYN *****S*
Nov 1 18:52:17 125.17.139.212:3074 -> 128.173.8.70:139 SYN *****S*
Nov 1 18:52:19 125.17.139.212:3089 -> 128.173.8.83:139 SYN *****S*
Nov 1 18:52:19 125.17.139.212:3101 -> 128.173.8.93:139 SYN *****S*
Nov 1 18:52:20 125.17.139.212:3128 -> 128.173.8.117:139 SYN *****S*
Nov 1 18:52:20 125.17.139.212:3136 -> 128.173.8.125:139 SYN *****S*

```

```

Nov 1 19:52:13 muddauber.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.44 PROTO=TCP
SPT=3046 DPT=139
Nov 1 19:52:14 hummingbird.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.62 PROTO=TCP
SPT=3064 DPT=139
Nov 1 19:52:15 muddauber.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.44 PROTO=TCP
SPT=3046 DPT=139
Nov 1 19:52:17 hummingbird.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.62 PROTO=TCP
SPT=3064 DPT=139
Nov 1 19:52:22 mosquito.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.183 PROTO=TCP
SPT=3203 DPT=139
Nov 1 19:52:22 muddauber.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.44 PROTO=TCP
SPT=3046 DPT=139
Nov 1 19:52:23 hummingbird.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.62 PROTO=TCP
SPT=3064 DPT=139
Nov 1 19:52:23 katydid.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.225 PROTO=TCP
SPT=3251 DPT=139
Nov 1 19:52:25 mosquito.cns.vt.edu SRC=125.17.139.212 DST=128.173.8.183 PROTO=TCP
SPT=3203 DPT=139

```

```

netstat -na
useradd dana
passwd dana
passwd dana
ifconfig
cd /home/
ls
cd dana/
ls
mv ssh-1.2.27.tar.gz /usr/local/src/
ls
cd /usr/local/src/
ls
tar -zxvf ssh-1.2.27.tar.gz
cd ssh-1.2.27
./configure
make
make install
ssh 172.18.0.1
which ssh
cd /usr/local/bin/
ls
exit
ssh
ssh 172.18.0.1
ifconfig
ssh 172.17.0.1
vi /etc/rc.d/rc.sysinit
reboot
vi /etc/sysconfig/network
vi /etc/hosts
vi /etc/sysconfig/network
vi /etc/hosts
reboot
shutdown -h now
shutdown -h now

```

/root/.bash History

Source of Attack ?

- Use tcpdump / who / syslog to see – from where they are coming in ?
- Run ‘finger’ against remote system
 - If ‘finger’ is working on attacker system you may be able to correlate activity with times of attack and user idle time
 - Usually attacker will be using a stolen account on remote machine
- Check NIC registry for attacker domain and *telephone* the site technical contact
 - Remember: your communications may be compromised

Security Issues

- Handling encrypted traffic
- Avoiding detection & circumvention
- Protecting sensitive data revealed by analysis

Law Enforcement Agencies (LEA)

- LEA's interest generally depends on the importance given to a case by media
- LEA & Judiciary : many still IT ignorant
- So are many of the Govt Ministries, Deptts and PSUs
- The situation may improve rapidly
 - But will depend on interest & location

References

- “Network Forensics: Tapping the Internet” by Simson Garfinkel (O'Reilly Network)
- “Lecture #14 - Network Forensics” by Bhavani Thuraisingham (University of Texas)
- “Experimentation in Network Forensics” by Naveen K Kumashi, et al (C-DAC, Bangalore)
- “Intrusion Detection & Network Forensics” by Marcus J Ranum
- “Forensics – Tools”; <http://www.forinsect.de/index.html>
- “Collecting Electronic Evidence After a System Compromise” by Matthew Braid (SANS Security Essentials)

References (contd..)

- “Computer Forensics – An Overview” by Dorothy A. Lunn (SANS Institute)
- http://www.giac.org/practical/gsec/Dorothy_Lunn_GS_EC.pdf
- “Manual for Investigation of Computer Related Crimes” by Ashok Dohare
- Course Contents : SANS SEC508
- HoneyNet Project Website – Computer Forensics Challenges
- “File System Forensic Analysis” by Brian Carrier (Addison Wesley)

Questions?

Thanks!