Network Forensics

Network based Attacks, Prevention & Allied Tools

Prof. Zaheed Shaikh
Department of Computer Engineering

Network Attacks

- Denial of service

  Denial of service attacks cause the service or program to cease functioning or prevent others from making use of the service or program.

- These may be performed at the network layer by sending carefully crafted and malicious datagrams that cause network connections to fail.
- They may also be performed at the application layer, where carefully crafted application commands are given to a program that cause it to become extremely busy or stop functioning.
- Preventing suspicious network traffic from reaching hosts and preventing suspicious program commands and requests are the best ways of minimizing the risk of a denial of service attack.
- It is useful to know the details of the attack method, so you should educate yourself about each new attack as it gets publicized.

Network Attacks

- Spoofing
  This type of attack causes a host or application to mimic the actions of another.
- Typically the attacker pretends to be an innocent host by following IP addresses in network packets.
- For example, a well-documented exploit of the BSD rlogin service can use this method to mimic a TCP connection from another host by guessing TCP sequence numbers.
- To protect against this type of attack, verify the authenticity of datagrams and commands.
- Prevent datagram routing with invalid source addresses. Introduce unpredictablility into connection control mechanisms, such as TCP sequence numbers and the allocation of dynamic port addresses.

Network Attacks

- Eavesdropping
  This is the simplest type of attack.
- A host is configured to "listen" to and capture data not belonging to it. Carefully written eavesdropping programs can take usernames and passwords from user login network connections.
- Broadcast networks like Ethernet are especially vulnerable to this type of attack.
- To protect against this type of threat, avoid use of broadcast network technologies and enforce the use of data encryption.
- IP firewalling is very useful in preventing or reducing unauthorized access, network layer denial of service, and IP spoofing attacks.
- It not very useful in avoiding exploitation of weaknesses in network services or programs and eavesdropping.

Securing a Network

- Need measures to secure a network and prevent breaches
- Apply patches; User a layered network defense strategy
- NSA (National Security Agency) has developed DiD Defense in Depth) and has three models of protection
  - People, Technology, Operations
  - People: Employees are trained well
  - Technology: Strong network architecture and testing tools
  - Operations: applying security patches, anti-virus software, etc.

Network Security Mechanisms

- Network security starts from authenticating any user, most likely a username and a password.
- Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network users
- Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.
- An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service.
- Communication between two hosts using the network could be encrypted to maintain privacy.
- Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Network Security Mechanisms

- Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools.
- Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.
- Such analysis could be used to further tighten security of the actual network being protected by the honeypot
- Some tools: Firewall, Antivirus software and Internet Security Software. For authentication, use strong passwords and change it on a bi-weekly/monthly basis. When using a wireless connection, use a robust password. Network analyzer to monitor and analyze the network.

Network Forensics

- What is Network Forensics?
  - http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci859579,00.html
- Network Forensics Analysis
- Relationship to Honeynets/Honeypots
- Policies for Networks Forensics
- Example Prototype System
- Some Popular Networks Forensics Analysis Tools (NFAT)

What is Network Forensics

- Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity.
  - Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.
- A network forensics appliance is a device that automates this process.
- Wireless forensics is the process of capturing information that moves over a wireless network and trying to make sense of it in some kind of forensics capacity.

What is Network Forensics?

- Network forensics systems can be one of two kinds:
  - *"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.
  - *"Stop, look and listen" systems*, in which each packet is analyzed 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.

What is Network Forensics

- Network Forensics is the process of collecting and analyzing raw network data and then tracking network traffic to determine how an attack took place
- When intruders break into a network they leave a trail. Need to spot variations in network traffic; detect anomalies
- Network forensics can usually help to determine whether network has been attacked or there is a user error
- Examiners must establish standards procedures to carry out forensics

Network Analysis

- Find analysis techniques developed for one type of network and apply it to another type of network
- Types of networks
  - Computer and Communication Networks
  - Telecommunication Network
  - Transportation networks
    - Highways, Railroad, Air Traffic
  - Human networks
    - Terror networks, Relationship networks

Network Forensics Analysis Tools (NFAT): Relationships between IDS, Firewalls and NFAT

- IDS attempts to detect activity that violates an organization's security policy by implementing a set of rules describing preconfigures 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
- NFATs must do the following:
  - Capture network traffic
  - Analyze network traffic according to user needs
  - Allow system users discover useful and interesting things about the analyzed traffic

NFAT Tasks

- Traffic Capture
  - What is the policy?
  - What is the traffic of interest?
  - Intermal/Externasl?
  - Collect packets: tcpdump
- Traffic Analysis
  - Sessionizing captured traffic (organize)
  - 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

Network Forensics: NetworkMiner

- NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows.
- NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.
- The purpose of NetworkMiner is to collect data (such as forensic evidence) about hosts on the network rather than to collect data regarding the traffic on the network.
- The main view is host centric (information grouped per host) rather than packet centric (information showed as a list of packets/frames).

Honeynets/Honeypots

- Network Forensics and honeynet systems have the same features of collecting information about computer misuses
- Honeynet system can lure attackers and gain information about new types of intrusions
- Network forensics systems analyze and reconstruct he 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.

Honeynet project

- Honeynet project was established to make information about network attacks and solutions widely available
- Objectives: Awareness, information, tools
- Attacks: distributed Denial of Service, Zero day attacks
- Honeypot is a computer set up to lure attackers
- Honeywalls are computers set up to monitor what is happening to the honeypots in the network

Policies: Computer Attack Taxonomy

- Probing
  - Attackers reconnaissance
  - Attackers create a profile of an organization's structure, network capabilities and content, security posture
  - Attacker finds the targets and devices plans to circumvent the security mechanism
- Penetration
  - Exploit System Configuration errors and vulnerabilities
  - Install Trojans, record passwords, delete files, etc.
- Cover tracks
  - Configure event logging to a previous state
  - Clear event logs and hide files

Policies to enhance forensics

- Retaining information
- Planning the response
- Training
- Accelerating the investigation
- Preventing anonymous activities
- Protect the evidence

Example Prototype System

- Network Forensics Analysis mechanisms should meet the following:
  - Short response times; User friendly interfaces
- Questions addresses
  - How likely is a specific host relevant to the attack? What is the role the host played in the attack? How strong are two hosts connected to the attack?
- Features of the prototype
  - Preprocessing mechanism to reduce redundancy in intrusion alerts
  - Graph model for presenting and interacting with th3 evidence
  - Hierarchical reasoning framework for automated inference of attack group identification

Example Prototype System: Modules

- Evidence collection module
- Evidence preprocessing module
- Attack knowledge base
- Assets knowledge base
- Evidence graph generation module
- Attack reasoning module
- Analyst interface module
- Reference
- http://delivery.acm.org/10.1145/1420000/1410238/a4-wang.pdf?key1=1410238&key2=9838895521&coll=GUIDE&dl=GUIDE&CFID=57276464&CFTOKEN=77054716
- https://www.dfrws.org/2005/proceedings/wang_evidencegraphs.pdf

Network Tools

- Network Forensics tools help in the monitoring of the network
- Example: the records that Ps tools generate can prove that an employee ran a program without permission
- Can also monitor machines/processes that may be harmful
- Problem is the attacker can get administrator rights and start using the tools
- Chapter 11 discusses tools for Windows and Linux

Some Popular Tools

- Raytheon's SilentRunner
  - Gives administrators help as they attempt to protect their company's assets
  - Collector, Analyzer and Visualize Modules
- Sandstorm Enterprise's NetIntercept
  - Hardware appliance focused on capturing network traffic
- Niksun's NetDetector
  - Its an appliance like NetIntercept
  - Has an alerting mechanism
  - Integrates with Cicso IDS for a complete forensic analysis

Network Forensics: Open Source Tools

- Open source tools
  - Wireshark
  - Kismet
  - Snort
  - OSSEC
  - NetworkMiner is an open source Network Forensics Tool available at SourceForge.
  - Xplico is an Internet/IP Traffic Decoder (NFAT). Protocols supported: HTTP, SIP, FTP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6

Network Forensics: Commercial Tools

- Deep Analysis Tools (data mining based tools)
  - E-Detective
  - ManTech International Corporation
  - Network Instruments
  - NIKSUN's NetDetector
  - PacketMotion
  - Sandstorm's NetIntercept
  - Mera Systems NetBeholder
  - InfoWatch Traffic Monitor

Network Forensics: Commercial Tools

- Flow-Based Systems
  - Arbor Networks
  - GraniteEdge Networks
  - Lancope http://www.lancope.com/
  - Mazu Networks http://www.mazunetworks.com/
- Hybrid Systems
  - These systems combine flow analysis, deep analysis, and security event monitoring and reporting.
  - Q1 Labs http://www.q1labs.com/

Performing Live Acquisitions

- Insert bootable forensics CD in the suspect system
- Keep a log of all the actions
- Send collected information to a network drive
- Copy the physical memory
- Determine if root kit is present; access system's firmware, - -
- Get forensics hash value of all files

Performing Live Acquisitions: Windows

- Setup NetCat listener to send the forensics data
- Load Helix CD in the CD-ROM drive
- Click appropriate buttons – System Information; Glad arrow etc
- Click Acquire Live Image if Widows System
- Connect to NetCat listener to send the collected data (e.g., enter IP address of NetCat listener)
- Click Incidence Response Tools
- Click on appropriate tools to collect data

Standard procedures

- Standard installation image, hash schemes (e.g., MD5, SHA-1)
- Fix vulnerabilities if intrusion is detected
- Retrieve volatile data (RAM, processes)
- Acquire compromised drive and make forensics image of it
- Compare forensics image and standard image and determine if anything has changed

Network Logs

- Network logs record traffic in and out of network
- Network servers, routers, firewalls record activities and events that move through them
- One ways is to run Tcpdump
- When viewing network log, port information can give clues about suspicious activity
- Use network analysis tool

Packet Sniffers

- Devices or software to monitor (sniff) traffic
- TCP/IP sniffers operate at the Packet level; in OSI operates at the Layer 2 or 3 level (e.g. Data link or Network layers)
- Some sniffers perform packet captures, some perform analysis and some perform both
- Tools exist for examining (i) packets with certain flags set (ii) email headers (iii) IRC chats

Summary

- Network Forensics is the process of collecting and analyzing raw network data and then tracking network traffic to determine how an attack took place
- Layered defense strategies to the network architecture
- Live acquisitions are needed to retrieve volatile items
- Standard procedure are needed to establish how to proceed after a network attack occurs
- By monitoring network traffic can establish normal operations; then determine if there is an anomaly
- Network tools used to monitor networks; but intruders can get admin rights to attack from the inside
- Tools are available for monitoring network traffic for both Windows and Linux systems
- Honeynet project enables people to learn latest intrusion techniques

Summary

- Network forensics is essentially about monitoring network traffic and determining if there is an attack and if so, determine the nature of the attack
- Key tasks include traffic capture, analysis and visualization
- Many tools are now available
- Works together with IDs, Firewalls and Honeynets
- Expert systems solutions show promise

Links

- https://www.dfrws.org/2005/proceedings/wang_evidencegraphs.pdf
- http://www.cs.fsu.edu/~yasinsac/Papers/MY01.pdf
- http://www.sandstorm.net/support/netintercept/downloads/ni-ieee.pdf
- http://www.giac.org/certified_professionals/practicals/gsec/2478.php
- http://www.infragard.net/library/congress_05/computer_forensics/network_primer.pdf
- http://dfrws.org/2003/presentations/Brief-Casey.pdf
- http://delivery.acm.org/10.1145/1070000/1066749/p302-ren.pdf?key1=1066749&key2=0512850911&coll=GUIDE&dl=GUIDE&CFID=36223233&CFTOKEN=49225512
- http://dfrws.org/