Network Forensics

Network Forensics Overview

Network Forensics Overview

- **Network forensics**
  - process of collecting and analyzing raw network data
  - Systematic tracking of incoming and outgoing traffic
    - To ascertain how an attack was carried out
    - To know how an event occurred on a network
- Network attacks are on the rise
  - More focus on this field
  - Increasing demand for skilled technicians
    - shortfall of 50,000 network forensics specialists
      - in law enforcement, legal firms, corporations, and universities

Network Forensics Overview

- Intruders leave trail behind
- Variations in network traffic can help you track intrusions
  - knowing your network's typical traffic patterns is important
- Determine the cause of the abnormal traffic
  - Internal bug
    - Untested patch, custom program, untested open-source program
  - Attackers

Network Forensics Overview

- Network forensics examiners
  - must establish **standard procedures** for how to acquire data after an attack or intrusion incident
- Network administrators
  - Must **find compromised machines**, get them offline, and restore them as quickly as possible to minimize downtime
- Follow standard procedures
  - To ensure that all compromised systems have been found
  - To ascertain attack methods- prevent them from happening again

Securing a Network

- **Applying latest Patch**

- **Layered network defense strategy**
  - Sets up layers of protection to hide the most valuable data at the innermost part of the network

- **Defense in depth (DiD)**
  - Similar approach developed by the NSA (National Security Agency)

Securing a Network

- **Defense in depth (DiD)**
  - Modes of protection
    - People (hiring and treatment)
    - Technology (firewalls, IDSs, etc.)
    - Operations (patches, updates)
- If one mode of protection fails, the others can be used to thwart the attack

Securing a Network

- **Defense in depth (DiD)**
  - People as a mode of protection
    - means organizations must hire well-qualified people
    - treat them well so that they have no reason to seek revenge
    - employees must be trained adequately in security procedures
    - They must be familiar with the organization’s security policy

Securing a Network

- **Defense in depth (DiD)**
  - The technology mode
    - Choose strong network architecture
    - Use tested tools
      - intrusion detection systems (IDSs)
      - Firewalls
    - Regular penetration testing coupled with risk assessment can help improve network security

Securing a Network

- **Defense in depth (DiD)**
  - Operations mode
    - Addresses day-to-day operations
    - Updating security patches, antivirus software, and OSs falls into this category
    - Assessment and monitoring procedures
    - Disaster recovery plans

Securing a Network

- Testing networks is as important as testing servers
- Need to be up to date on the latest methods intruders use to infiltrate networks
- Inside attacker

Performing Live Acquisitions

Performing Live Acquisitions

- Useful when dealing with active network intrusions or attacks
- Done before taking a system offline
- It is becoming a necessity
  - Because Live acquisition, affect RAM and running processes
  - Attacks might leave footprints only in running processes or RAM
  - information in RAM is lost after you turn off a suspect system.
  - Some malware disappears after a system is restarted

Performing Live Acquisitions

- **Order of volatility (OOV)**
  - How long a piece of information lasts on a system
    - Data such as RAM and running processes might exist for only milliseconds
    - Files stored on the hard drive, might last for years

Performing Live Acquisitions

- Steps - general procedure for a live acquisition
  - Create or download a live-acquisition forensic CD
  - Make sure you keep a log of all your actions
  - A network drive is ideal as a place to send the information you collect; an alternative is a USB disk
  - Copy the physical memory (RAM)
  - The next step varies: search for rootkits, image the drive over the network, or shut down for later static acquisition
  - Be sure to get a forensic hash value of all files you recover during the live acquisition

Performing a Live Acquisition in Windows

- Several tools are available to capture the RAM.
  - Mantech Memory DD
  - Win32dd
  - winen.exe from Guidance Software
  - BackTrack

Developing Standard Procedures for Network Forensics

Developing Standard Procedures for Network Forensics

- Long, tedious process
- Standard procedure
  - Always use a standard installation
  - Fix vulnerability after attack
  - Attempt to retrieve all volatile data
  - Acquire all compromised drives and make a forensic image
  - Compare files on the forensic image to the original installation image

Developing Standard Procedures for Network Forensics

- Computer forensics
  - Work from the image to find what has changed
- Network forensics
  - Restore drives to understand attack
- Work on an isolated system
  - Prevents **malware** from affecting other systems

Reviewing Network Logs

- Record ingoing and outgoing traffic
  - Network servers
  - Routers
  - Firewalls
- Tcpdump tool for examining network traffic
  - Can identify patterns

Using Network Tools

Using Network Tools

- Variety of tools are available for network administrators to perform remote shutdowns, monitor device use
- Sysinternals
  - A collection of free tools for examining Windows products
- Examples of the Sysinternals tools:
  - RegMon shows Registry data in real time
  - Process Explorer shows what is loaded
  - Handle shows open files and processes using them
  - Filemon shows file system activity

Using Network Tools

- Tools from PsTools suite created by Sysinternals
  - PsExec runs processes remotely
  - PsGetSid displays security identifier (SID)
  - PsKill kills process by name or ID
  - PsList lists details about a process
  - PsLoggedOn shows who’s logged locally
  - PsPasswd changes account passwords
  - PsService controls and views services
  - PsShutdown shuts down and restarts PCs
  - PsSuspend suspends processes

Using UNIX/Linux Tools

- Knoppix Security Tools Distribution (STD)
  - Bootable Linux CD intended for computer and network forensics
- Knoppix-STD tools
  - Dcfldd, the U.S. DoD dd version
  - memfetch forces a memory dump
  - photorec grabs files from a digital camera
  - snort, an intrusion detection system
  - oinkmaster helps manage your snort rules

Using UNIX/Linux Tools

- Knoppix-STD tools
  - john
  - chntpw resets passwords on a Windows PC
  - tcpdump and ethereal are packet sniffers
- With the Knoppix STD tools on a portable CD
  - You can examine almost any network system

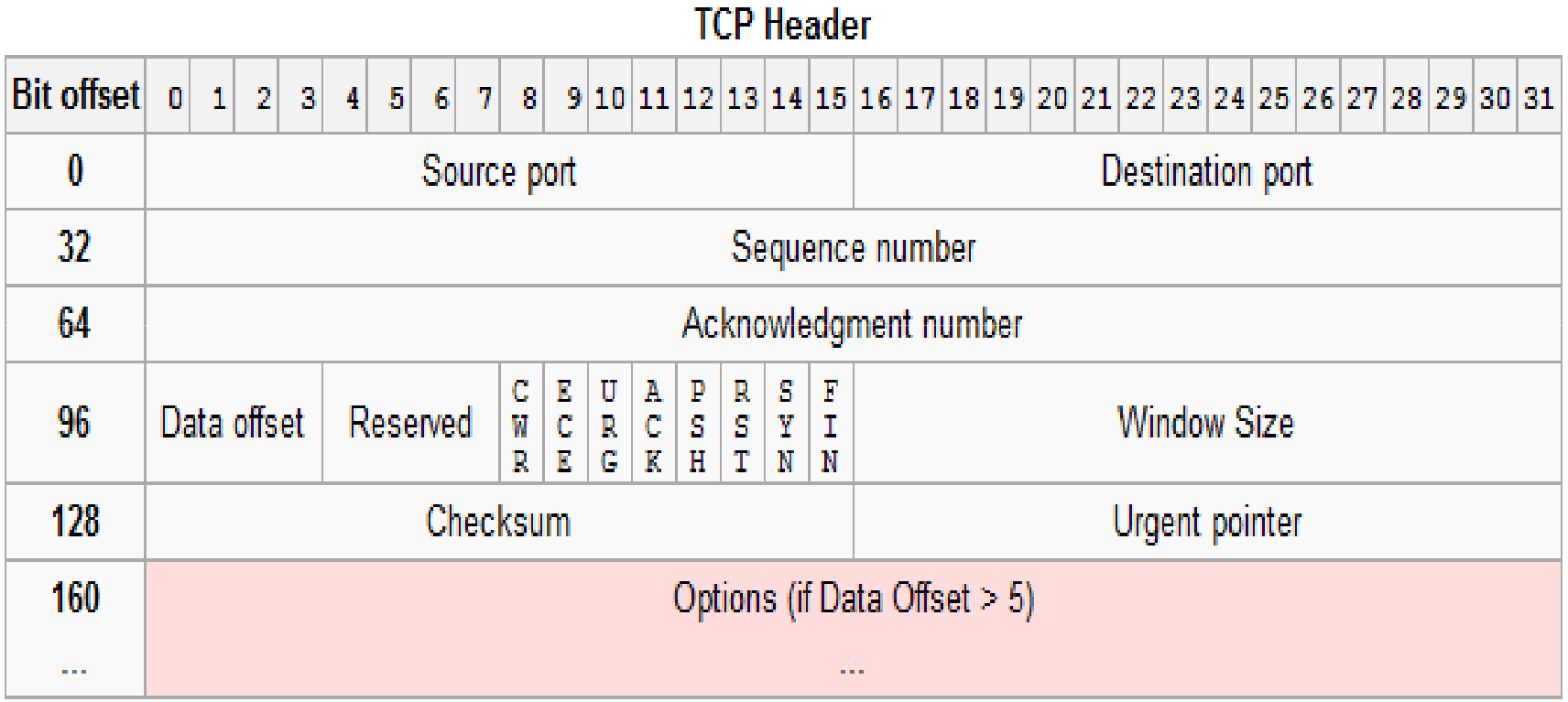
Using UNIX/Linux Tools

- BackTrack
  - Contains more than 300 tools for network scanning, brute-force attacks, Bluetooth and wireless networks, and more
  - Includes forensics tools, such as Autopsy and Sleuth Kit
  - Easy to use and frequently updated

Using Packet Sniffers

- Packet sniffers
  - Devices or software that monitor network traffic
  - Most work at layer 2 or 3 of the OSI model
- Most tools follow the PCAP format
- Some packets can be identified by examining the flags in their TCP headers

TCP Header


TCP Header
Bit offset
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0
Source port
Destination port
32
Sequence number
64
Acknowledgment number
96
Data offset
Reserved
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Window Size
128
Checksum
Urgent pointer
160
...
Options (if Data Offset > 5)
...

Tools

- Tcpdump (command-line packet capture)
- Tethereal (command-line version of Ethereal)
- Wireshark (formerly Ethereal)
  - Graphical packet capture analysis
- Snort (intrusion detection)
- Tcpslice
  - Extracts information from one or more tcpdump files by time frame

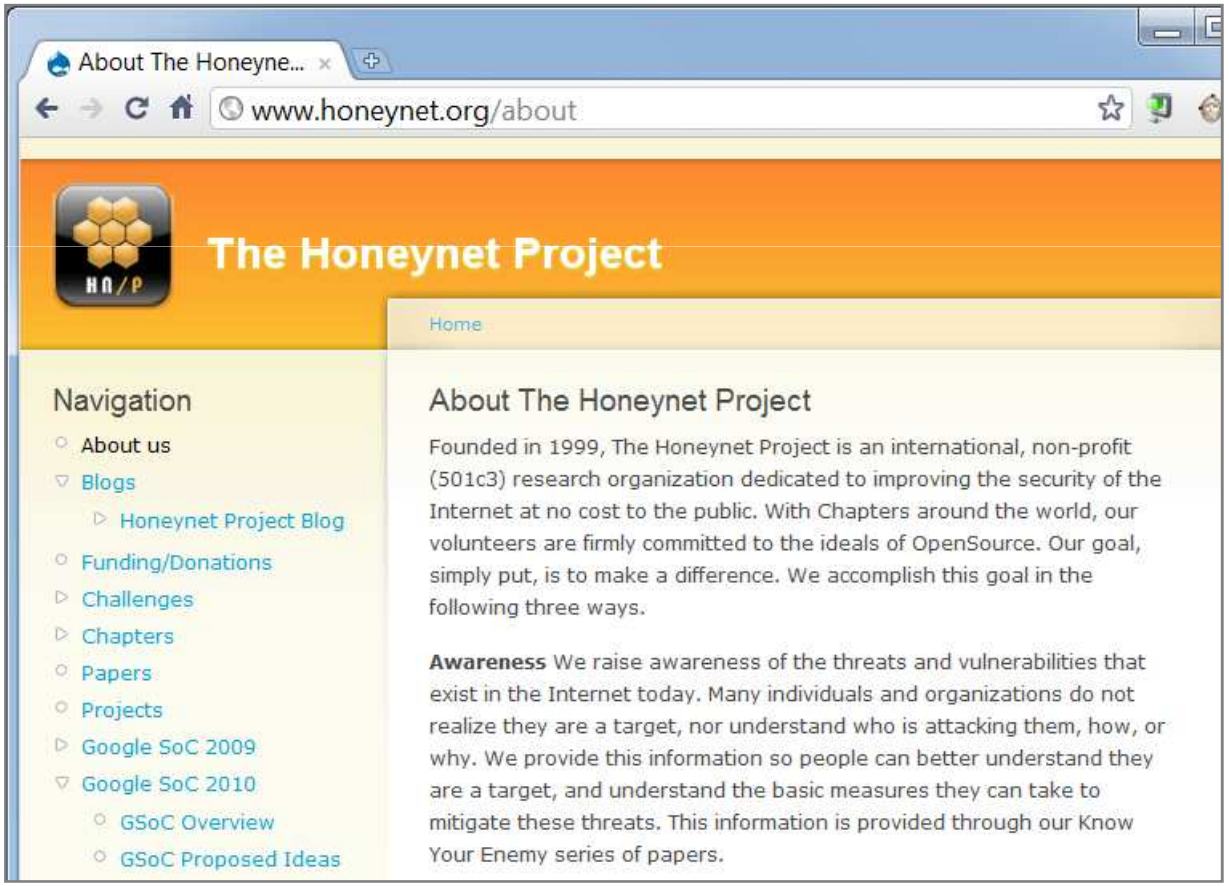
Tools

- Tcpreplay (replays packets)
- Tcpdstat (near-realtime traffic statistics)
- Ngrep (pattern-matching for pcap captures)
- Etherape (views network traffic graphically)
- Netdude (GUI tool to analyze pcap files)
- Argus (analyzes packet flows)

Examining the Honeynet Project

- Attempt to thwart Internet and network hackers
  - Provides information about attacks methods
- Objectives are awareness, information, and tools
- **Distributed denial-of-service (DDoS) attacks**
  - A recent major threat
  - Hundreds or even thousands of machines (**zombies**) can be used

Examining the Honeynet Project



Examining the Honeynet Project

- **Zero day attacks**
  - Another major threat
  - Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available
- Honeypot
  - Normal looking computer that lures attackers to it
- Honeywalls
  - Monitor what’s happening to honeypots on your network and record what attackers are doing

Examining the Honeynet Project

- Its legality has been questioned
  - Cannot be used in court
  - Can be used to learn about attacks
- Manuka Project
  - Used the Honeynet Project's principles
    - To create a usable database for students to examine compromised honeypots
- Honeynet Challenges
  - You can try to ascertain what an attacker did and then post your results online