Network-based Intrusion Detection

Tom Chen
SMU
tchen@engr.smu.edu

Outline

- Introduction
- Types of Malicious Traffic
- Traffic Monitoring
- Traffic Analysis
- Real-Time Intrusion Detection

Introduction

Recent Cases

- 20-year old hacker on trial now in California for breaking into US government computers in April 2004
  - Claimed goal was to expose security weaknesses of classified military computers
  - Used default passwords to break into MS SQL servers, and password cracking tools
- Faces up to 16 years prison

Recent Cases (cont)

- June 24 discovered Russian hackers had broken into various Web servers
  - Exploited vulnerability in Microsoft IIS (Internet Information Server), part of Windows2000 server
  - Installed malicious Javascript code into the Web servers to redirect surfers to computers run by the hackers

Recent Cases (cont)

  - Javascript code exploits a vulnerability in Internet Explorer

- Hackers' computer secretly downloaded keystroke logger on surfer's PC to steal passwords and credit card data, and uploads to hackers' Website
- Unknown exact identities of hackers or exact goal in stealing private data

Recent Cases (cont)

- July 30 Microsoft released patch for 3 “critical” vulnerabilities in Internet Explorer
  - Critical means an attack could possibly gain complete control of PC
- Vulnerabilities related to the IE vulnerability exploited by Russian hackers in June

Recent Cases (cont)

- July 18 Bagle.AI and MyDoom.N worms spread by email
  - Bagle.AI is attachment in short email message from fake sender and subject line "Re:"
  - MyDoom.N is also attachment in message from "Postmaster" or "Mailer-daemon", appears to be a rejected message from mail server

Recent Cases (cont)

- July 26 latest MyDoom.O worm added capability to search for email addresses using a search engine
  - When worm finds an email address on infected PC, it searches for other addresses in same domain using Google or Lycos
  - Sends copy of itself to these addresses

Why Computers Are Targets

- Servers store confidential data for businesses, individuals, governments, military
- Software have many vulnerabilities (eg, Windows) easy to exploit
  - Automated attack tools are easy to find
- Networks (esp. Internet) allow easy remote access

Why Computers (cont)

- Electronic data can be easily copied
- Attacks across network can be hard to trace
- Broadband home PCs (cable modems) are often unprotected and always connected to Internet

Common Vulnerabilities

- Computers and networks are left on default configurations (default passwords)
- Computers and networks are misconfigured
- Software vulnerabilities are continually discovered - about average 7 new vulnerabilities per day (according to Symantec)

Types of Intruders

- Professionals
  - Industrial spies
  - Organized crime
  - Military intelligence
- Amateur hackers
  - Typically young men
  - Maybe acquaintances

Intruder Goals

- Intruders have various motives: profit, espionage, revenge, extortion, fame, fun
- At same time, intruders believe risk is low
  - Law enforcement must be able to trace intruder through network
  - Legal prosecution requires hard evidence and proof of motive
  - Many countries have weak laws

Types of Attacks

Direct attacks to access computers

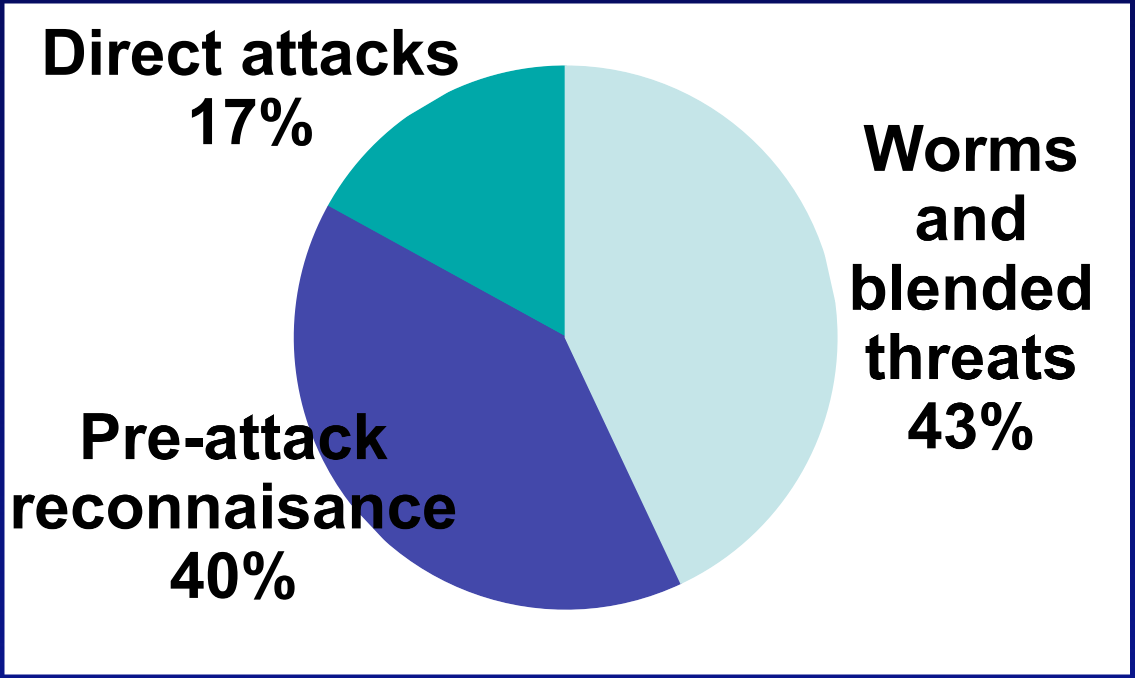
- Phase 1: reconnaisance
- Phase 2: exploit
- Phase 3: avoid detection

Large-scale attacks on the network

- Harmful effects on the entire network
- Purpose is damage, not control
- Viruses, worms, denial of service

Types of Attacks

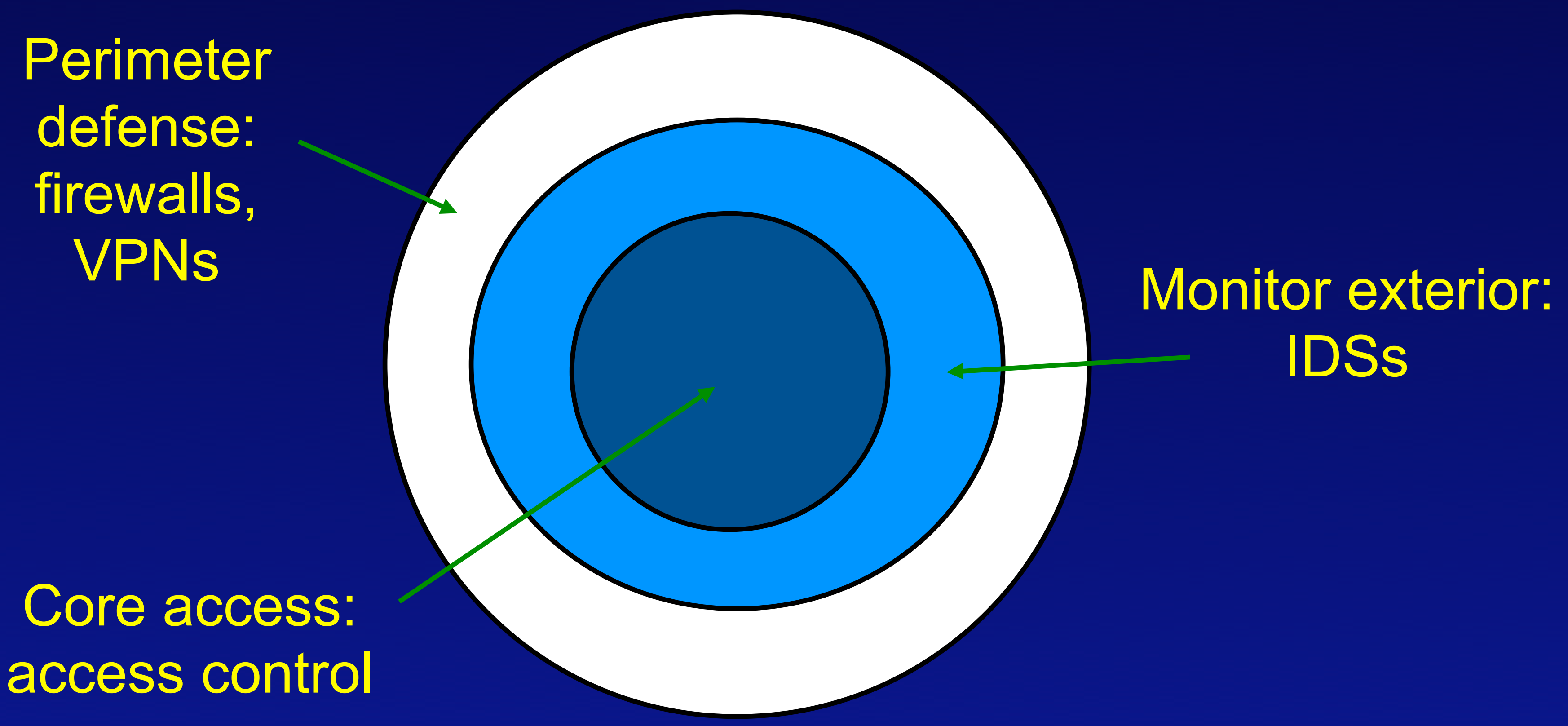
- Symantec Report 2003:



Role of Intrusion Detection

- Intrusion detection systems (IDSs) are part of typical "defense in depth" strategies
  - Various security components form layers of protection against attacks
  - Goal is not perfect protection, but make attackers spend more effort (cost)

Defense in Depth



Role of Intrusion Detection

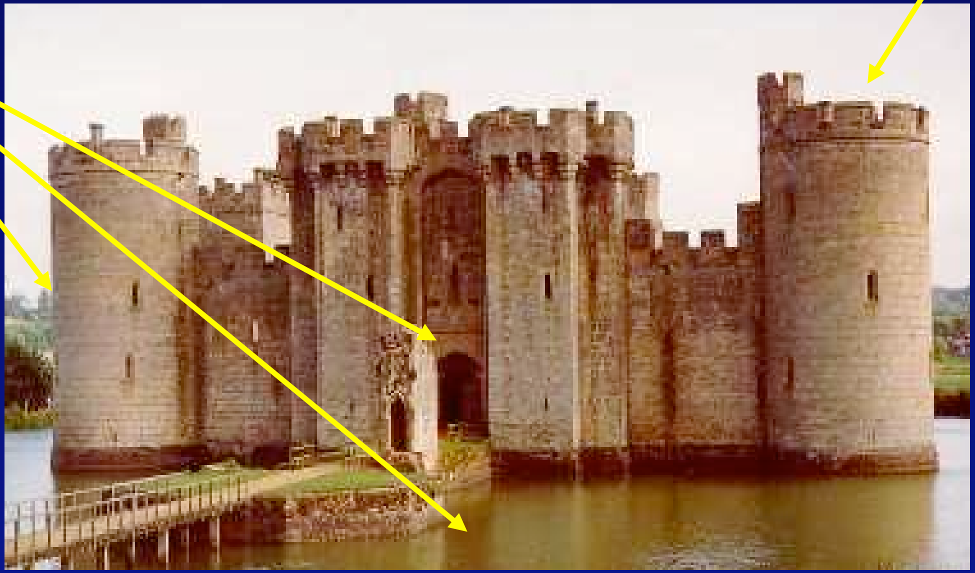
- By analogy, castle is protected by walls, locked doors, moat, vault -- preventive layers
- IDSs serve as burglar alarms and watch guards -- reactive layer
  - Useful complement to preventive layers

Role of Intrusion Detection

- Castle analogy

Walls, moat, gate keep intruders out

Guards and alarms look out for suspicious activities



History of IDSs

- 1980 James Anderson wrote report for US Air Force, proposed a method for processing computer audit trails to detect unusual usage patterns using statistical analysis
- 1986 Dorothy Denning and Peter Neumann developed real-time IDES (Intrusion Detection Expert System) for US Navy

History (cont)

- Anomaly detector characterized statistics of abnormal behavior
- Expert system applied rules to detect security violations

- 1990 U. of California-Davis developed NSM (Network System Monitor), first IDS to analyze network traffic

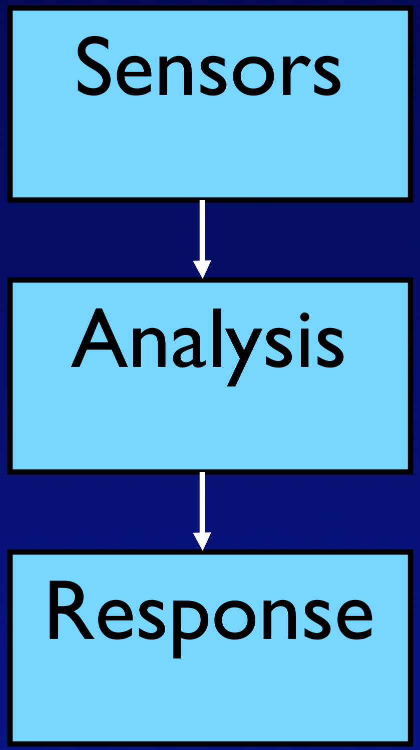
History (cont)

- 1992 DIDS (Distributed Intrusion Detection System) was large-scale R&D project between various US research labs and military agencies
  - In response to 1988 Morris worm
  - Goal to integrate IDSs across networks to centrally track security violations and intrusions

History (cont)

- 1990s commercial IDSs sold
- 1998 DARPA sponsored an Intrusion Detection Evaluation of many IDSs
- Today IDSs are evolving into intrusion prevention systems (IPS)
  - IPS takes an active response after detected intrusion

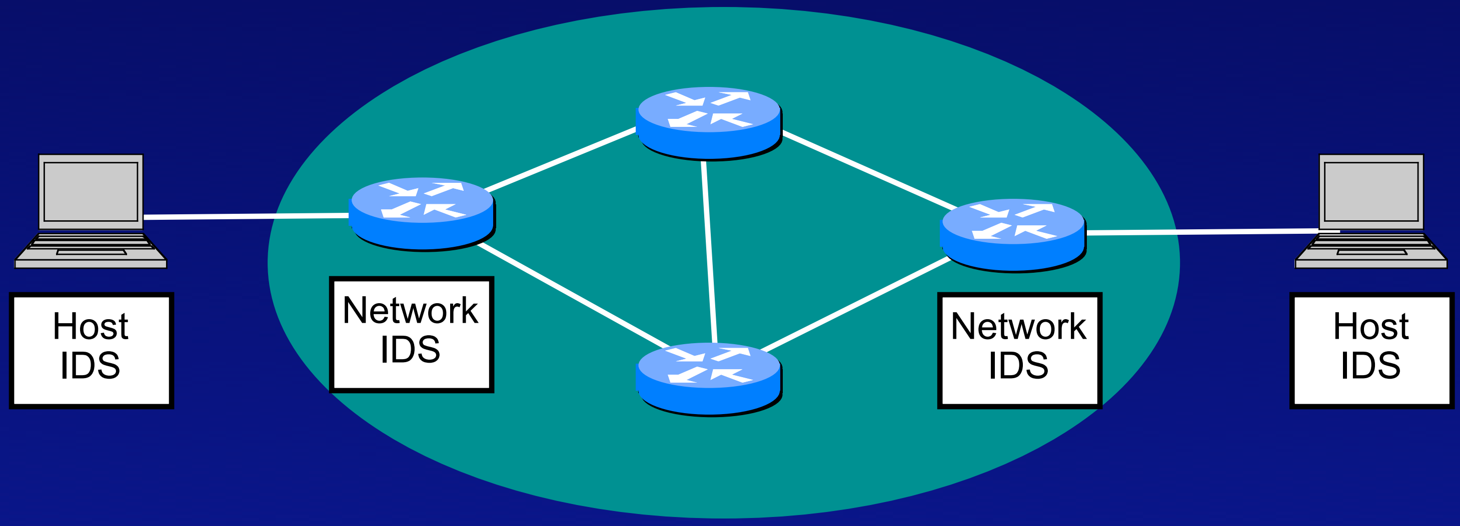
IDS Basic Functions



- Continually monitor activities (packet traffic or host behavior)
- Recognize suspicious, malicious, or inappropriate activities
- Trigger alarms to system administrator

Types of Intrusion Detection

- Intrusion detection can be classified as host-based or network-based



Types of IDSs (cont)

- Host-based IDS: monitor host activities (audit trails)
  - Most reliable detection, but does not scale well (with increasing number of hosts)
- Network-based IDS: monitor packet traffic
  - Scalable but detection accuracy is a difficult problem

Types of Malicious Traffic

Types of Attack Traffic

Direct attacks to access computers

- Reconnaisance (scanning)
  - Not really malicious
- Exploits (buffer overflows, password attacks, Trojan horses)

Large-scale attacks on the network

- Viruses, worms, denial of service, spam

Phase 1 - Reconnaissance

- Attackers often prepare for attacks by first collecting information about targets - look for weakest defense point
- Info. includes IP addresses, map of routers and servers, email addresses, modem dialup numbers, operating system details, open ports, login names, system vulnerabilities, maybe passwords

Reconnaisance - Mapping

- Tools: Sam Spade, CyberKit, NetScanTools, iNetTools, Cheops
- Ping (ICMP echo request) sweeps will identify IP addresses of active hosts
  - Or TCP SYN packets can be used
- Traceroute used to map routers around target machine

Reconnaisance - Scanning

- Port scanners: Nmap, Strobe, Ultrascan, Netcat, SuperScan, WinScan
- Port scanning at well known TCP/UDP ports reveals services running on targets
  - TCP 80 = HTTP, UDP 53 = DNS, TCP 25 = SMTP
- Also, some ports are known used for backdoors, Trojan horses, spyware

Recon - Fingerprinting

- Fingerprinting is to figure out details of target's operating system
  - Different vulnerabilities depend on OS
- TCP protocol is standardized but responses to illegal TCP packets are not
  - Operating systems respond differently to TCP packets with illegal flags
  - Nmap can identify 500+ OS fingerprints

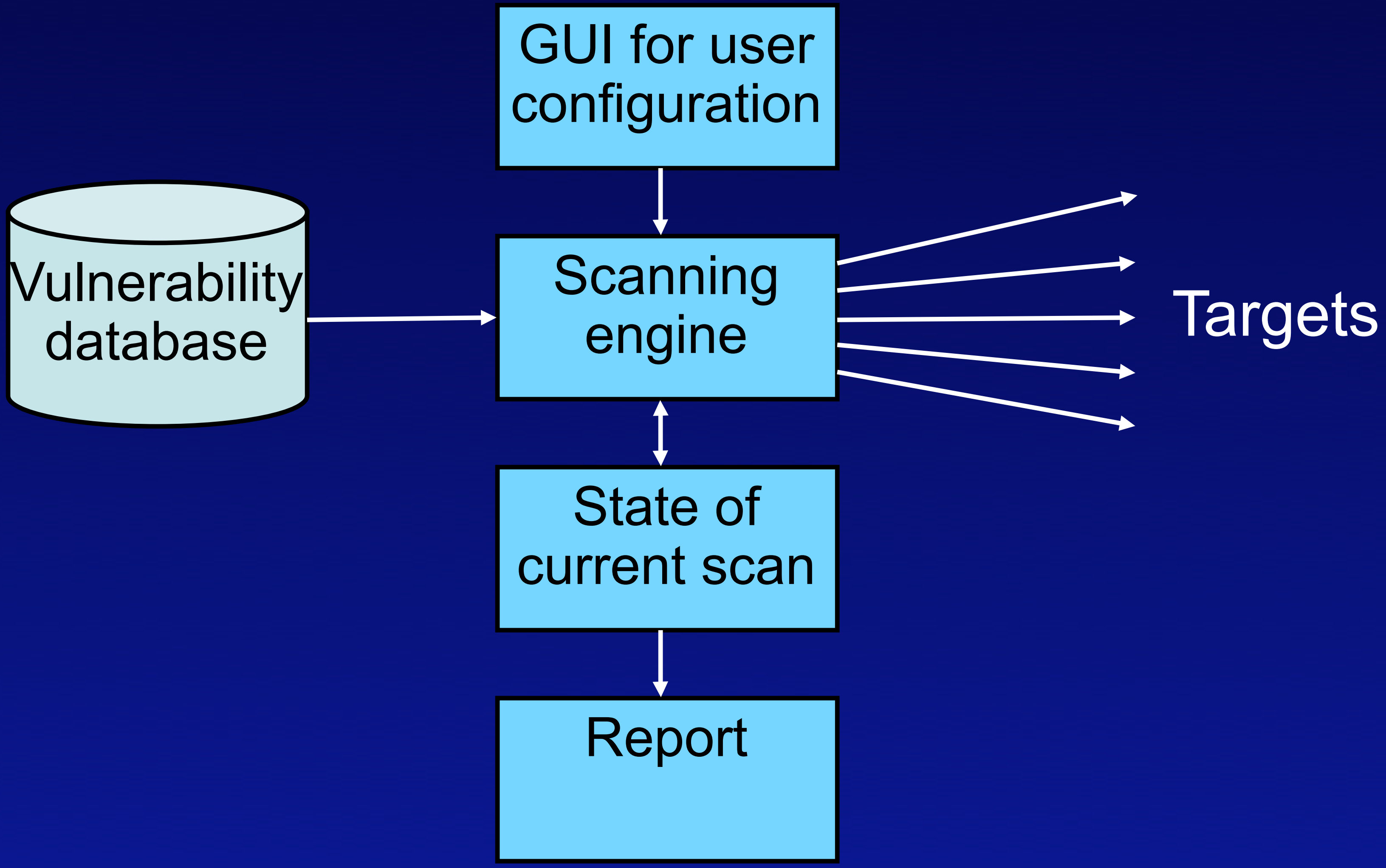
Recon - Firewall Scanning

- Tool: Firewalk
- First finds IP address of firewall, then number of hops to reach firewall (traceroute)
- Then learns which packets are allowed through firewall by sending packets with TTL = one hop past firewall

Recon - Vulnerability Scans

- Tools: Nessus, SARA, SAINT, VLAD, CyberCop Scanner, NetRecon, Retina Scanner
- Tools check for
  - Common configuration errors
  - Default security settings (default passwords)
  - Published vulnerabilities

Vulnerability Scanner



Phase 2 - Exploit

- Password attack tools: L0phtCrack, John the Ripper, Crack, Pandora
- Password attacks are easy to carry out, often successful
  - Passwords are often names (50%), sports words (30%), common words (11%)
  - Vulnerable to dictionary attack
  - People tend to re-use same password

Password Attacks (cont)

- Routers, switches, operating systems often ship with default passwords not changed by system administrators
  - List of default passwords is easy to find:
  - `www.phenoelit.de/dpl/index.html`

Password Attacks (cont)

- Password cracking:
  - Many systems store user IDs and passwords encrypted in password file
  - Steal password file, then run password cracking tool (tries guess, encrypts guess, matches with password file)

Phase 2 - Exploit (cont)

- Buffer overflow attack is very common because easy to do, and can give complete control over target
  - Most common exploit used by worms
  - Buffer overflow vulnerabilities are found in many systems and applications, especially those written in C (because C is weak on checking bounds of variables)

Buffer Overflow (cont)

- Buffer overflow happens when more data than expected is accepted, overflowing into the stack
  - If done carefully, attacker can make any program code run on target computer
  - Attacks can be carried out remotely through network

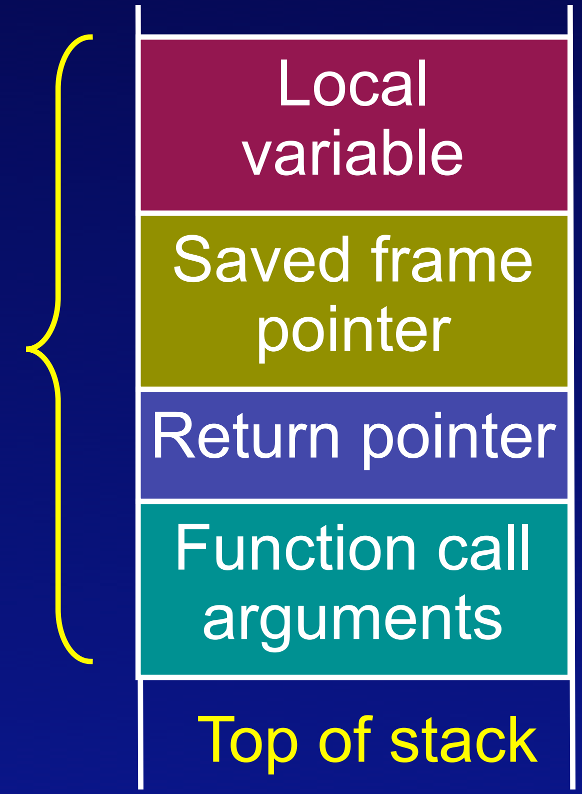
Buffer Overflow (cont)

Program

```
main()
    {
    function(data);
    printf("..");
    }
```

Push onto stack for function call

Stack



Buffer Overflow (cont)

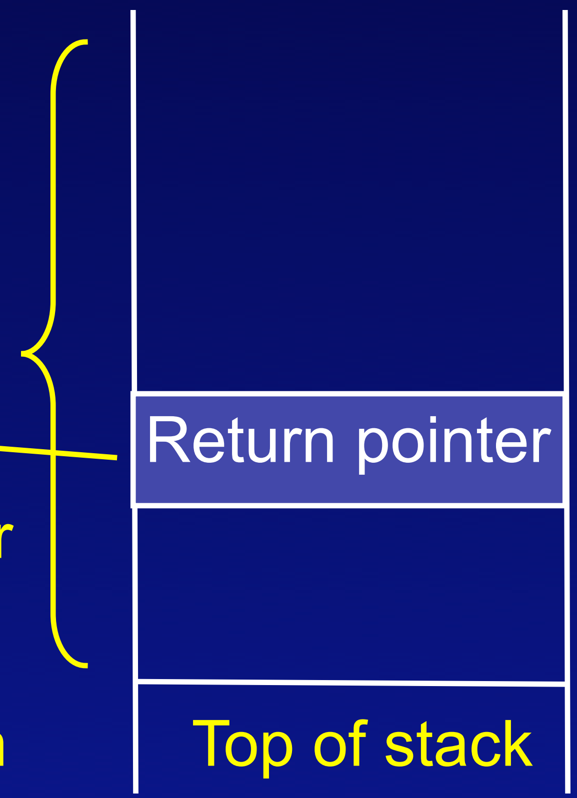
Program

```
main()
    {
    function(data);
    printf("..");
    }
```

Pop off stack after function call

Return pointer resumes execution in main program

Stack



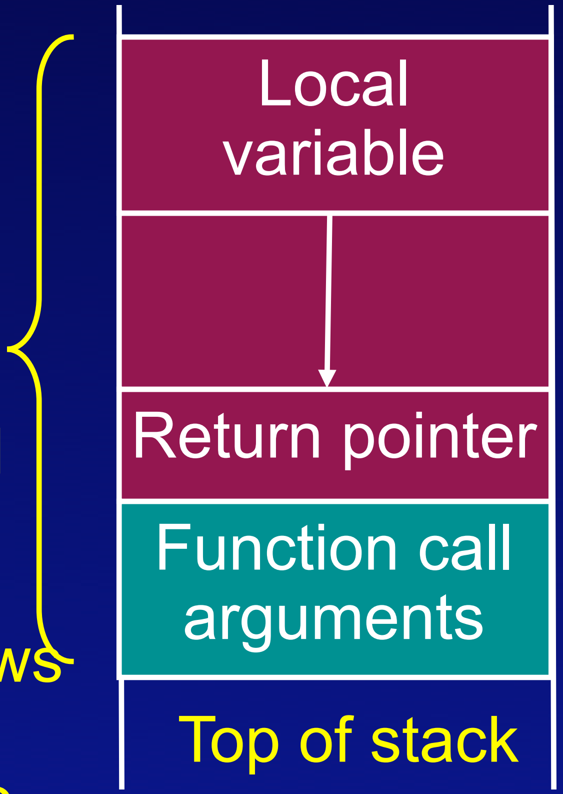
Buffer Overflow (cont)

Program

```
main()
    {
    function(data);
    printf("..");
    }
```

Buffer overflow attack

When pushed on stack, data for local variable overflows buffer and overwrites into return pointer



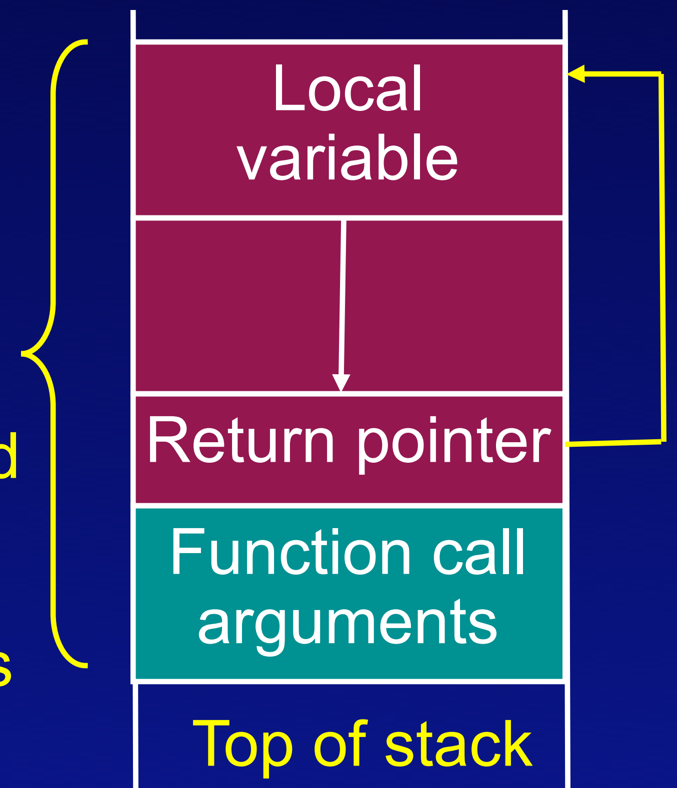
Buffer Overflow (cont)

Program

Buffer overflow attack

```
main()
    {
    function(data);
    printf("..");
    }
```

When popped off stack, new return pointer points into buffer to run attacker's code



Buffer Overflow (cont)

- Buffer overflow attack needs to know exactly how to overflow buffer ("smash the stack")
  - Depends on processor and OS, so not easy to write
  - But exploit codes already written are easy to find and re-use

Phase 2 - Exploit (cont)

- Social engineering attacks trick users into compromising their security
  - Typically email message tricks users to open attachment (can be virus or Trojan horse) or visit a Web site
- Recent phishing attacks: email pretending to be from bank or credit card tells user to verify their account at fake Web site that looks like real Web site

Phase 2 - Exploit (cont)

- Many exploits try to install Trojan horses (malicious program that appears to do something useful, or hide themselves as invisible file or innocent file)
  - Trojans can be installed by social engineering (tricking user), email attachment, or viewing Web site
  - Examples: NetBus, Back Orifice, Sub7, Optix, Net-Devil (…hundreds more)

Trojan Horses (cont)

- Trojans can do anything, usually spying or damage
  - Most Trojans open backdoor (allow secret remote access) -- called RATs (remote access Trojans)
  - Also, keyloggers (capture all keystrokes) and other spyware steal private data
    - Usually send data by email to hacker

Viruses and Worms

- Viruses and worms do not try to control specific computers
- Purpose is to spread as far and quickly as possible
- Viruses are pieces of code attached to normal programs or files
  - Depend on users to execute normal program, then virus code takes over execution and makes copies of itself

Viruses and Worms (cont)

- Worms are automated programs that spread through network
  - Exploit any vulnerabilities to compromise another computer and send a copy of itself
  - Often choose random IP addresses to target
  - Fast scanning can cause traffic surges, even serious congestion

Viruses and Worms (cont)

- In addition to congestion effects, viruses and worms can deliver any payloads to infected computers
  - Common payloads are Trojan horses or denial of service agents

Denial of Service (DoS)

- Most DoS attacks use
  - Malformed packets (e.g., Land, Teardrop, ping of death) to crash the target
  - Packet flooding (e.g., SYN flood, Smurf attack) to exhaust the target resources
- Packet flooding now typically carried out in distributed DoS (DDoS) attacks

DDoS (cont)

- DDoS tools: TFN, TFN2K, Trin00, Stacheldraht
- 2 phases:
  - Many machines are compromised with secret Trojan horse (DoS agent) - called zombies or bot network - maybe by virus or worm
  - Zombies flood target when instructed

Spam

- Zombies (bot networks) are increasingly used for spam
- Spam originated as annoying junk email, but now combined with viruses, Trojan horses, social engineering -- more dangerous
- Spammers' goal is profit

Spam (cont)

- Low cost to send flood of email, so even very small fraction of success can result in profit
- Spam filters typically look for word patterns in email, current accuracy 95 -99 percent
  - Spammers continually invent new ways around filters

Traffic Monitoring and Data Collection

Legal Limitations

- Traffic is monitored constantly by various points in network
  - Servers, routers, firewalls, intrusion detection systems
  - Traffic can reveal much personal data
- Normally privacy is protected by laws

US Wiretap Act (Title 18)

- 1968 passed to prevent illegal wiretapping phone calls
- Legal wiretaps require judge to approve a court order for a probable cause and specific individual

Types of Wiretaps

- Pen register captures destination phone numbers
- Trap-and-trace captures origin phone numbers
  - Neither captures the conversation
  - Requires court order like full wiretap, but not probable cause

ECPA

- 1986 ECPA (Electronic Communications Privacy Act) extended Wiretap Act to cover illegal eavesdropping on all electronic communications, although most people know email is unsecure
- Legal eavesdropping requires a court order for a specific individual and probable cause

Types of Electronic Wiretaps

- Pen register and trap-and-trace extend to packet communications
- Court orders allow capture of email headers, source/destination IP addresses of packets, web URLs

CALEA

- 1994 CALEA (Communications Assistance for Law Enforcement Act) passed to help FBI
- Requires phone companies and Internet service providers to use networks that support legal wiretapping
- Phone companies and ISPs must assist FBI or police given a wiretap order

USA Patriot Act

- Passed after September 11, 2001 terrorist attacks on New York City and Pentagon
- Relaxes limitations on US government to carry out electronic surveillance
- Allows higher penalties for computer crimes

Sniffers

- Sniffer tools: Snort, Ethereal, Dsniff
- Packet sniffers are computers with network interface cards in “promiscuous mode” to receive all packets on LAN or wireless LAN
  - Widely used, easy, free, reliable
- Sniffers can be placed on switched networks if switches have mirrored port

Server Logs

- Servers typically log data about transactions
  - Source/destination IP addresses, transaction time, service-dependent info.
  - Most useful are Web and email servers

Routers - NetFlow

- Cisco high-end routers have NetFlow feature
- Records flows, retrievable by network managers
  - Source/destination address, start/stop time, number of packets, total data, source/destination autonomous system numbers, input/output router ports, TCP flags, ICMP type

Firewalls

- Firewalls are mainly to filter traffic but they keep log data about incoming/ outgoing connections
  - Source/destination IP addresses, time, port numbers, action taken and reason, packet length, protocol, direction

Intrusion Detection Systems

- Equipment designed to monitor traffic, recognize patterns of suspicious or malicious traffic, raise alarms
- Many free and commercial IDSs
- Can be host-based or network-based
  - Network-based IDS can be integrated in routers or firewalls
- IDS logs are similar to firewall logs

Honeypots and Honeynets

- Honeypots are decoy PCs that intentionally look vulnerable to attackers
- Assigned unused IP address that should see no legitimate traffic, so traffic to honeypot is probably malicious
- Set up to monitor and record all activities
  - Goal to learn about attackers' behavior

Honeypots (cont)

- Cheap and useful, but must wait for attack traffic to that IP address
- More advanced variations:
  - Honeynet is a network of complete (regular) computers, set up to attract attacks but doing nothing else
  - Black hole network is block of unused IP addresses, to monitor incoming traffic

Traffic Analysis

Data Outputs

- Different equipment will output data at different granularity
  - Packets - eg, sniffers, honeypots
  - Flows - routers, firewalls
  - Sessions - firewalls, IDSs
  - Events - IDSs
- Granularity of sniffers, firewalls, and IDSs depends on filter rules

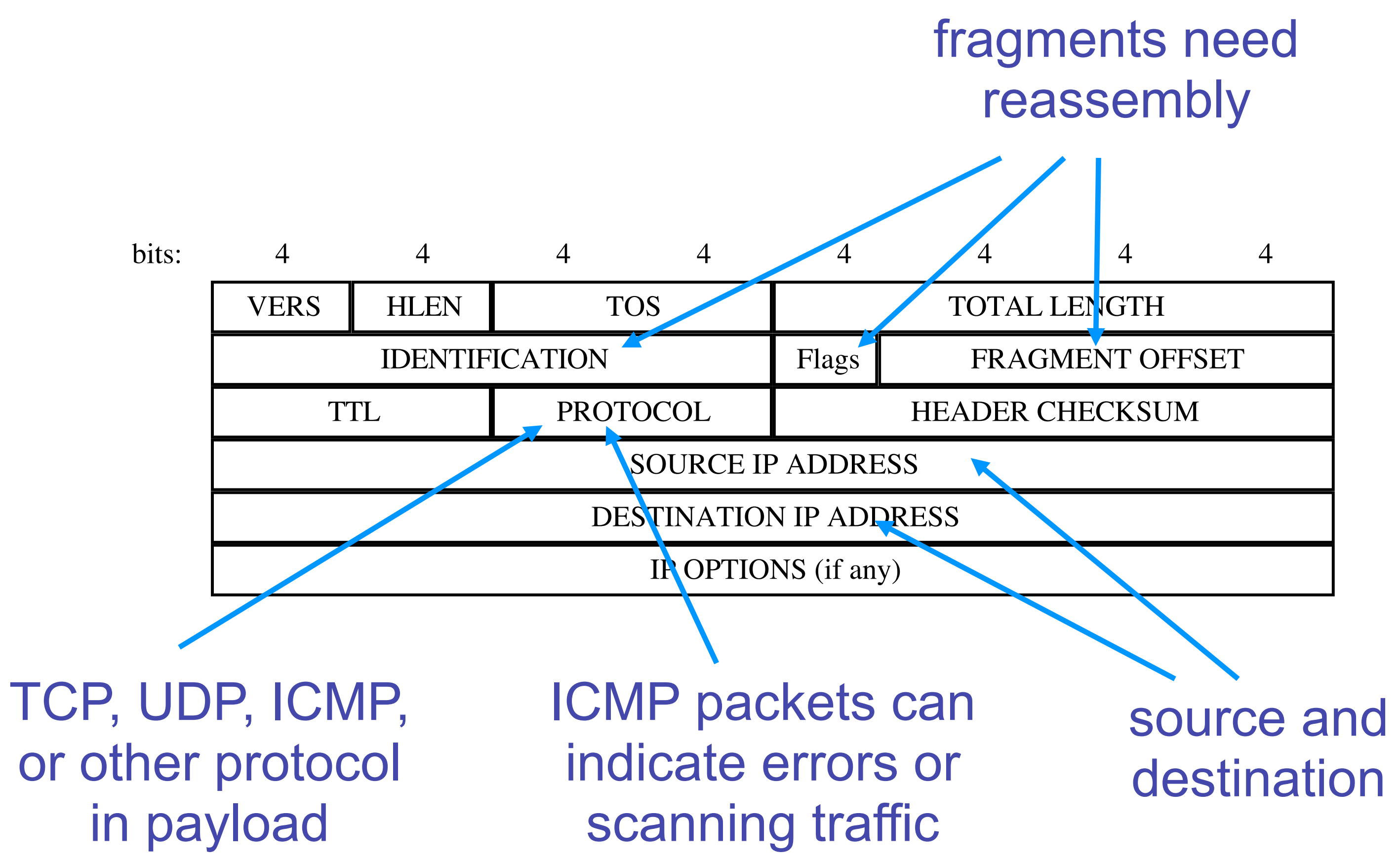
Data Reduction

- Network equipment can collect enormous volumes of data, not all interesting
- Useful to configure filter rules for sniffers and IDSs to look for only events of interest
- Or traffic data can be filtered by traffic analysis tools

Sessions Reconstruction

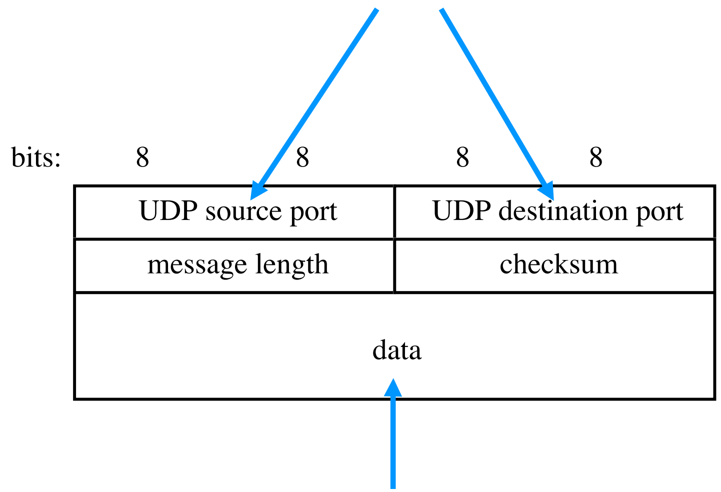
- Sessions can be reconstructed looking at IP, ICMP, UDP, TCP header fields in packet data
  - Identify when, where, and how connections are made, and ICMP errors
- Higher layer processing (email, Web) possible with deeper packet inspection

IP Header Analysis



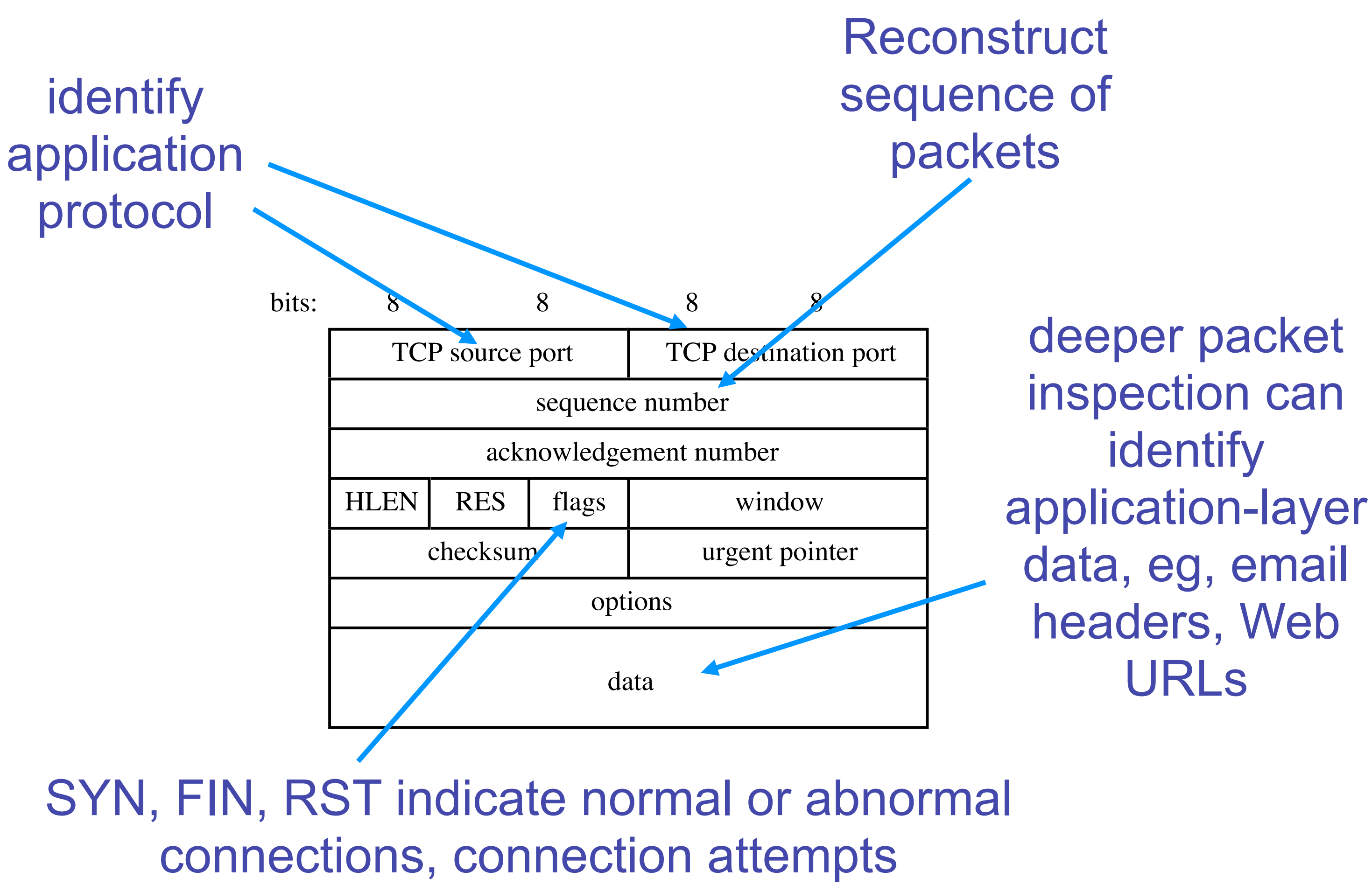
UDP Header Processing

identify application protocol



deeper packet inspection can identify application-layer data, eg, SNMP messages

TCP Header Processing

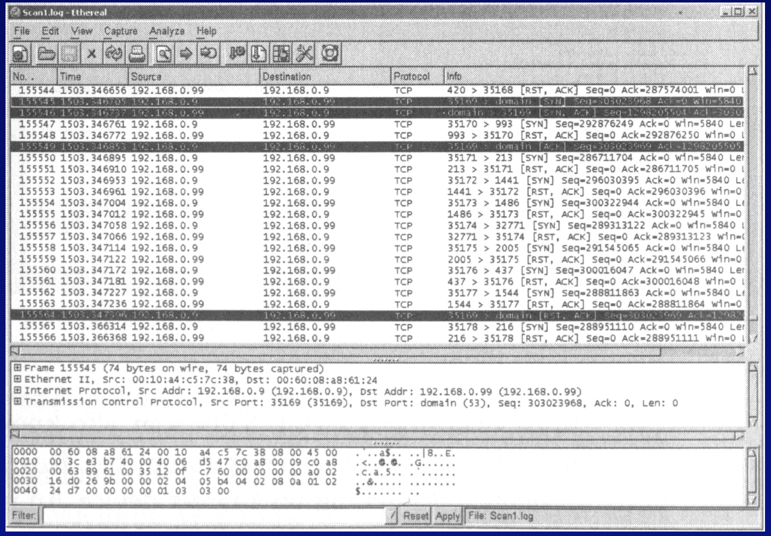


Traffic Analysis Tools

- Tcptrace and Tcpflow can reconstruct TCP/UDP sessions from packet data
- Snort can be configured with rules to filter out any info, look for events
- Ethereal is highly configurable and can reconstruct TCP sessions
- Dsniff can sniff and display email or Web sessions

Ethereal Examples

- Ethereal GUI



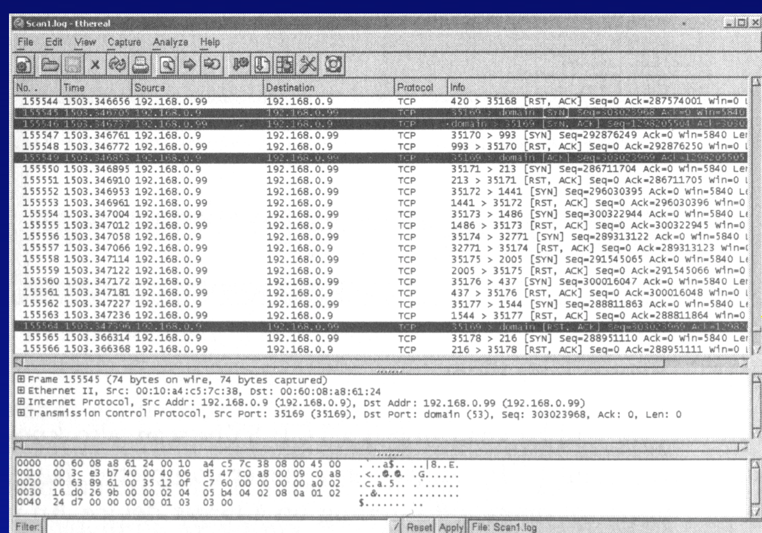
List of packets

Protocol details

Raw data

Ethereal Examples

- TCP connect scan
  - Repeated TCP SYN requests to different ports

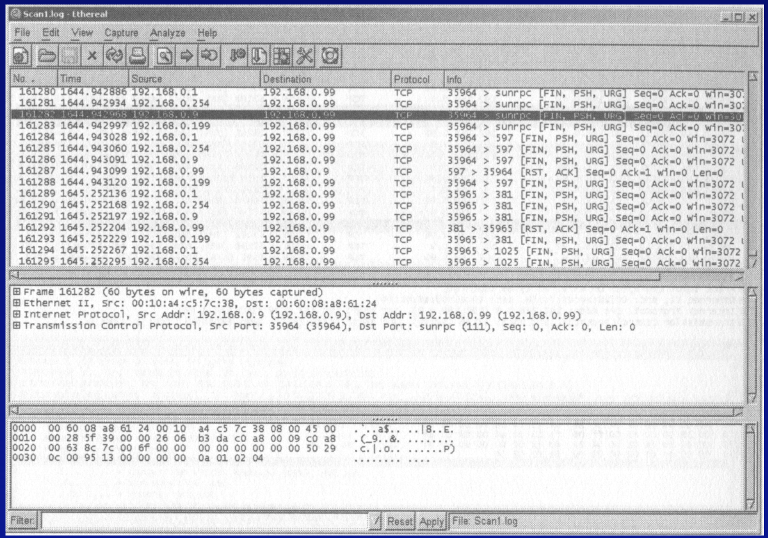


Open ports reply with SYN/ACK

Closed ports reply with RST/ACK

Ethereal Examples

- Xmas scan
  - Repeated TCP SYN requests with FIN, PSH, URG flags set

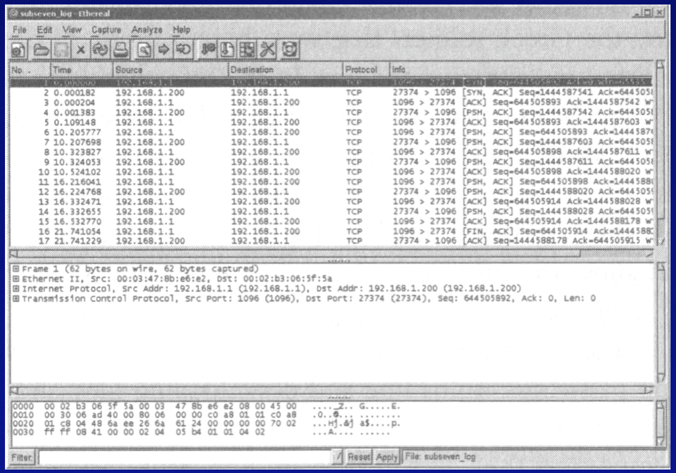


Open ports do not reply

Closed ports reply with RST/ACK

Ethereal Examples

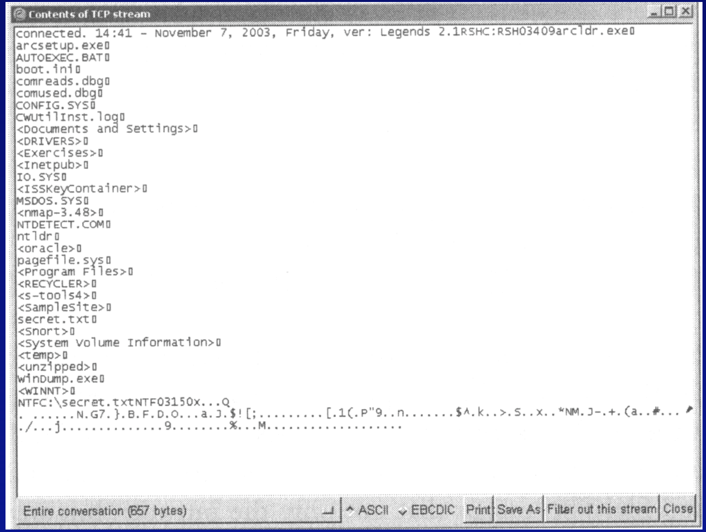
- Sub7 Trojan horse
  - Uses backdoor TCP connection to intruder on port 27374 by default



Many TCP packets through port 27374

Ethereal Examples

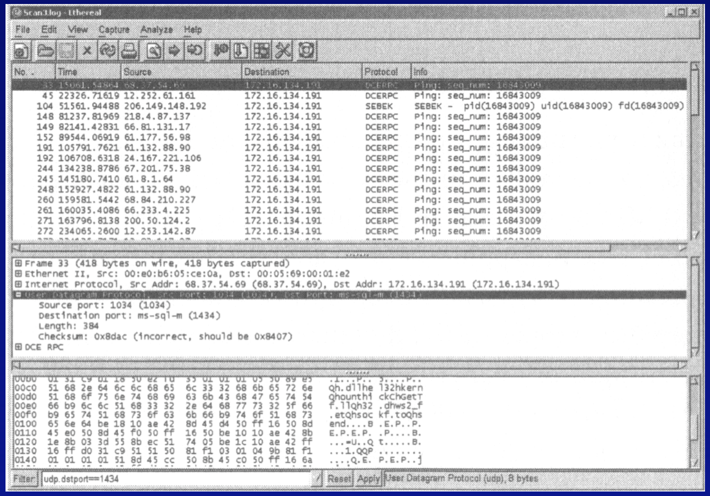
- Sub7 Trojan horse (cont)
  - Ethereal shows contents of TCP session



Intruder listed files in C: directory, and downloaded file "secret.txt"

Ethereal Examples

- SQL Slammer worm
  - Spreads by sending UDP packets to random IP addresses on port 1434



Many incoming UDP packets to port 1434

Real-Time Intrusion Detection

Challenges of Real-Time IDS

- Processing at wire speed (transmission link rate)
- Automated recognition of suspicious traffic
- Accuracy is main problem
  - Low false positives (false alarms)
  - Low false negatives (missed alarms)

Types of IDSs (cont)

- IDSs can also be classified in two approaches
  - Misuse (signature-based) detection
  - Anomaly (behavior-based) detection

Misuse Detection

- Most common approach
- Traffic data is compared to set of signatures (patterns) for known attacks
  - Alarm if a signature matches
- Definition of signatures is critical
  - If signatures are incomplete or too broad -- result in **false negatives** or **false positives**

Misuse Detection (cont)

- Disadvantages:
  - Signatures must be constantly updated for new attacks
  - New attacks will likely be missed if no signature -- potentially high **false negatives** (missed alarms)

Anomaly Detection

- Any behavior outside of a “normal profile” is considered suspicious
  - Normal behavior is defined in statistical terms
- Potential to detect new types of attack that are different from “normal” behavior, without need for a signature

Anomaly Detection (cont)

- Disadvantages:
  - Very difficult to define normal behavior in practice (too much variation)
  - Non-normal behavior may be suspicious but not malicious -- tend to high **false positives** (false alarms)
  - Additional processing needed to identify malicious (not just suspicious) activities

Detecting New Attacks

- Major research problem is accurate detection of new attacks
- Zero-day exploits are attacks on new vulnerability before signature is available
- Most commercial IDS systems use combination of misuse detection (signatures) and anomaly detection (ad hoc behavior rules)

Detecting New Attacks (cont)

- Problems:
  - Detection accuracy -- minimize false negatives and false positives
  - Determine intention -- identify malicious attacks in suspicious traffic (might be very small part)
  - Too many (false) alarms for system administrators

Intrusion Prevention Systems

- Intrusion prevention systems (IPS) is combination of IDS and active response
- Active responses could include
  - Blocking or slowing down traffic
  - Redirecting traffic to restricted environment
- Active responses could harm legitimate traffic -- detection accuracy is critical

Conclusions

- Real-time intrusion detection is difficult on-going research problem
- Main challenges are
  - How to detect new zero-day exploits
  - How to reduce high rate of alarms to truly malicious attacks
  - What active responses are appropriate