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

- 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

- 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

- 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

- July 18 Bagle.Al 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

- 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

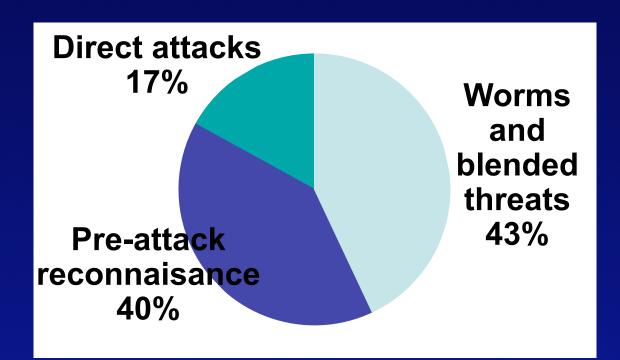
- Phase 1:
 reconnaisance
- Phase 2: exploit
- Phase 3: avoid detection

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

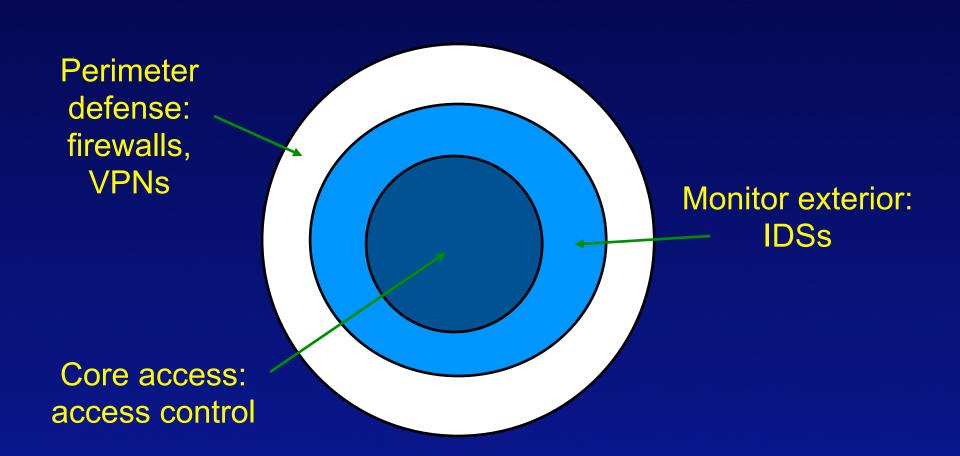
• Symantec Report 2003:



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

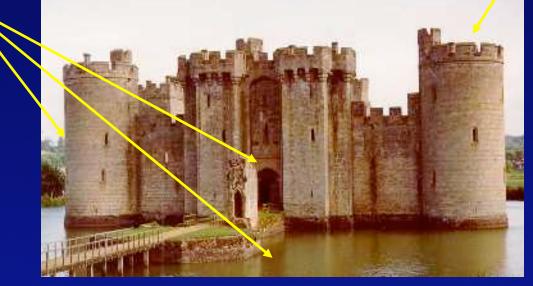
- By analogy, castle is protected by walls, locked doors, moat, vault -- preventive layers
- IDSs serve as burglar alarms and watch guards -- reactive layer
 - Useful complement to preventive layers

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

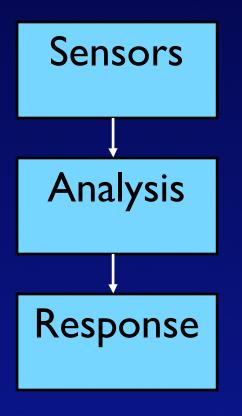
History (cont)

- 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

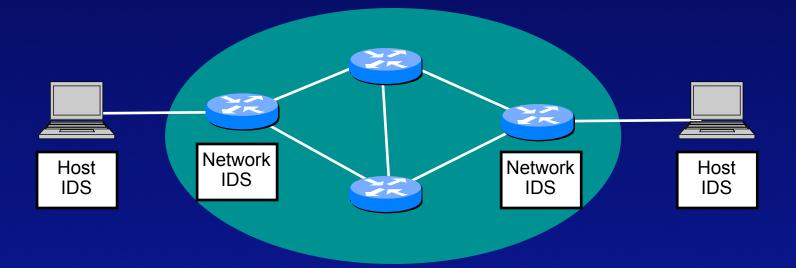
IDS Basic Functions



- 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

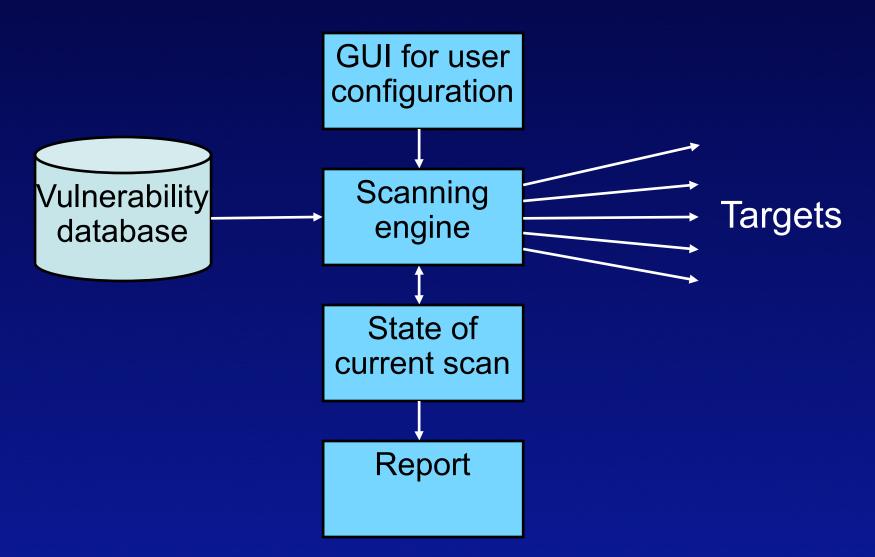
Recon - Firewall Scanning

- 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

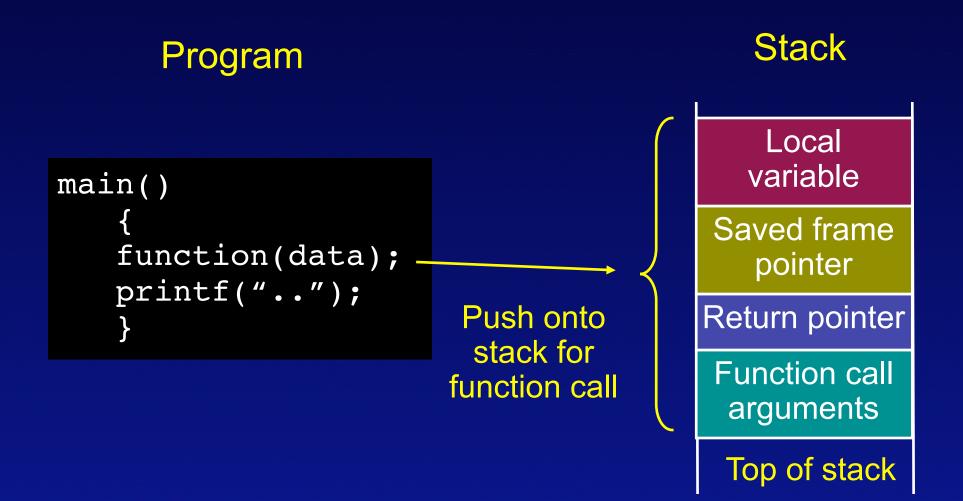
Password Attacks (cont)

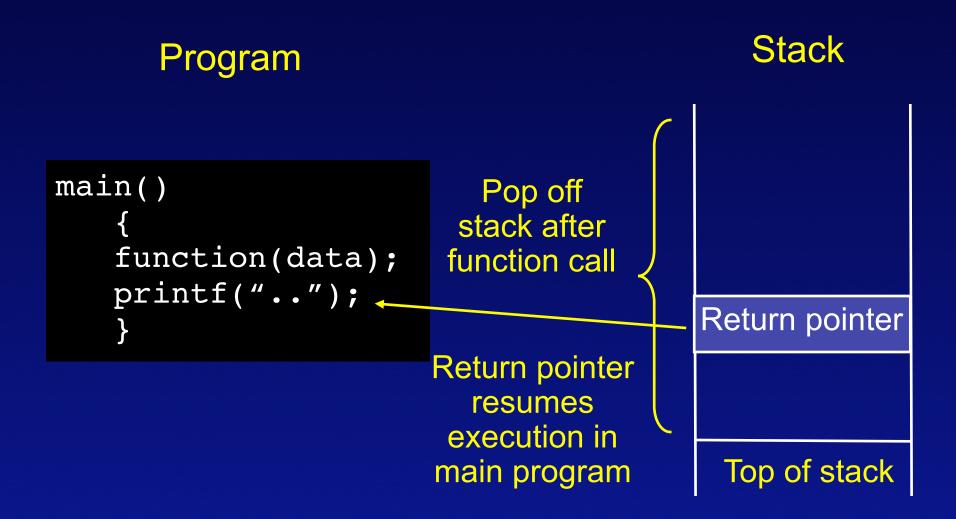
- Password cracking:
 - Many systems store user IDs and passwords encrypted in password file
 - Steal password file, then run password cracking tool (tries guess, encrypts guess, matches with password file)

Phase 2 - Exploit (cont)

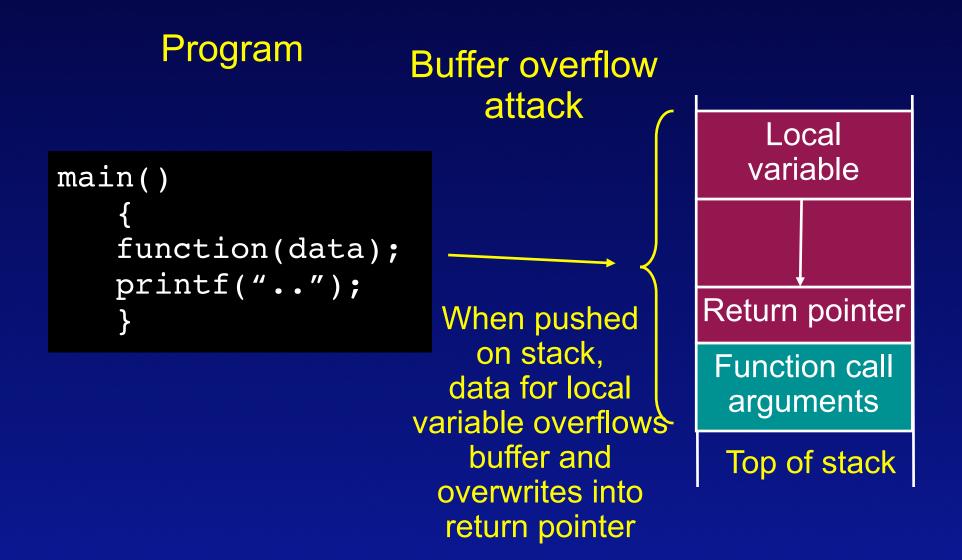
- Buffer overflow attack is very common because easy to do, and can give complete control over target
 - Most common exploit used by worms
 - Buffer overflow vulnerabilities are found in many systems and applications, especially those written in C (because C is weak on checking bounds of variables)

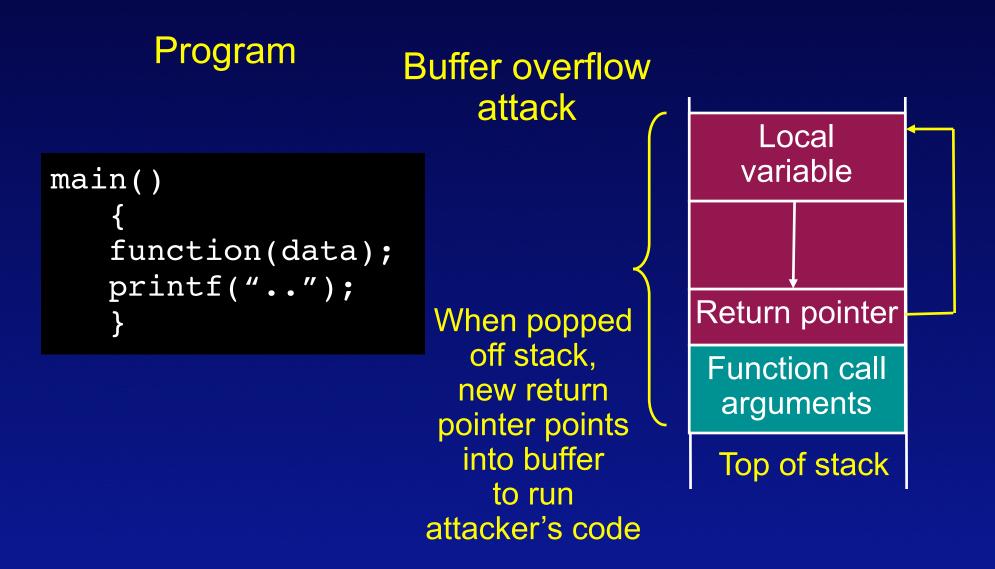
- Buffer overflow happens when more data than expected is accepted, overflowing into the stack
 - If done carefully, attacker can make any program code run on target computer
 - Attacks can be carried out remotely through network





TC/BUPT/8-7-04





- 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

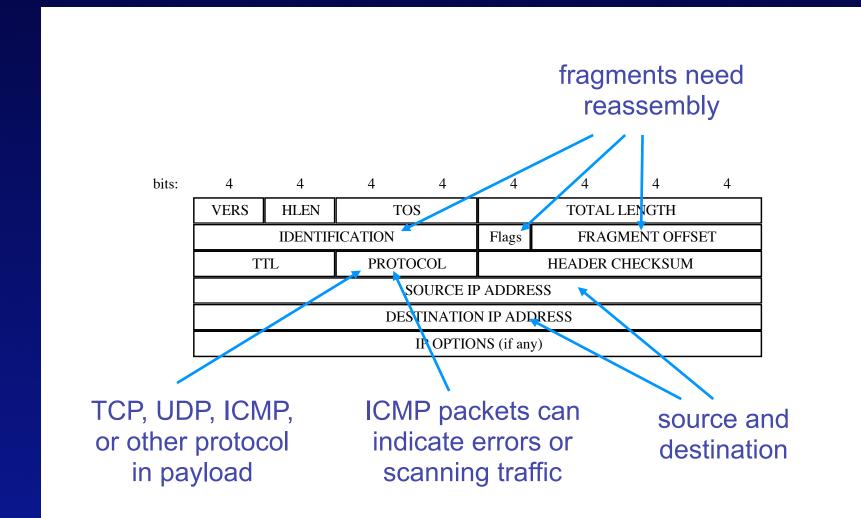
Data Reduction

- 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

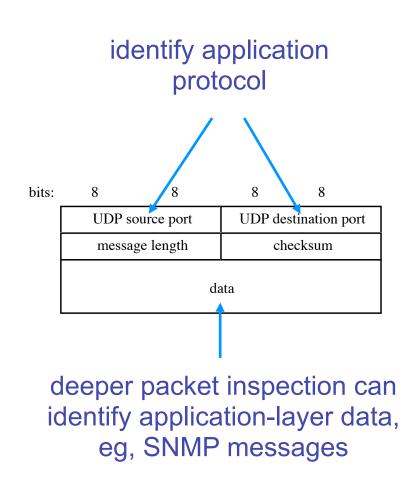
Sessions Reconstruction

- 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

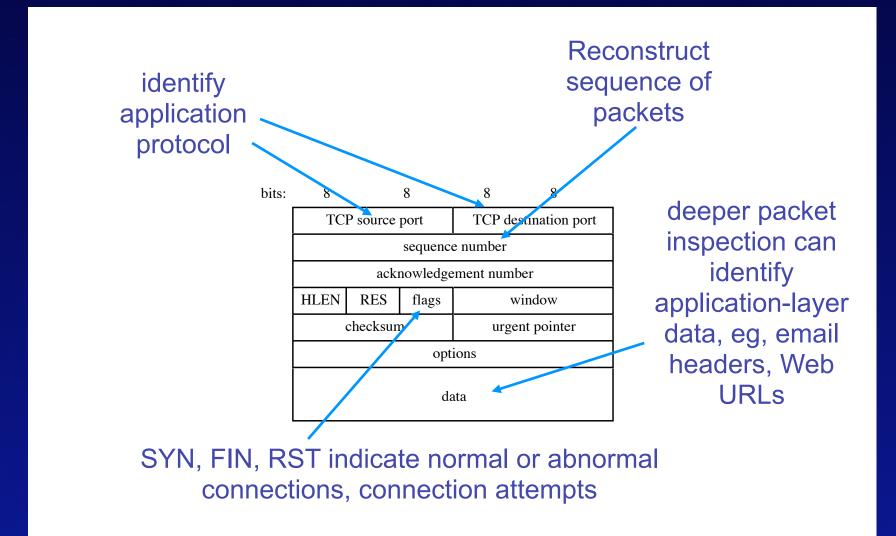
IP Header Analysis



UDP Header Processing



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 GUI

🖓 Scant.le	ig - Ethereal	a second and a second			الد •	JX		
File Ed	t View Capti	ure Analyze Help						
	🗐 x 😔		DBXQ					
No	Time	Source	Destination	Protocol	Info	77		
155544		192.168.0.99	192.168.0.9	TCP	420 > 35168 [RST, ACK] Seq=0 Ack=287574001 win=0			
	1503.346737	192.168.0.9 192.168.0.99	192.168.0.99 192.168.0.9	TCP	-domain > 35169 [SrN, ACK] Seq=1298205504 Adk=303	8 10		
		192.168.0.9 192.168.0.99	192.168.0.99 192.168.0.9	TCP TCP	35170 > 993 [SYN] Seq=292876249 Ack=0 win=5840 Lu 993 > 35170 [RST, ACK] Seq=0 Ack=292876250 win=0			
		192.168.0.99	192.163.0.99	TCP	35169 > domain [ACK] Seq=303023969 Ack=129820550	5		
		192.168.0.9	192.168.0.99	TCP	35171 > 213 [SYN] Seq=286711704 Ack=0 win=5840 L	er		
		192.168.0.99	192.168.0.9 192.168.0.99	TCP	213 > 35171 [RST, ACK] Seq=0 Ack=286711705 win=0 35172 > 1441 [SYN] Seq=296030395 Ack=0 win=5840 u			
		192.168.0.99	192.168.0.9	TCP	1441 > 35172 [RST, ACK] Seq=0 Ack=296030396 win=	0		List of packets
		192.168.0.9	192.168.0.99	TCP	35173 > 1486 [SYN] Seq=300322944 Ack=0 win=5840			I ICT OT DACKATC
		192.168.0.99	192.168.0.9 192.168.0.99	TCP	1486 > 35173 [RST, ACK] seq=0 Ack=300322945 win= 35174 > 32771 [SYN] seq=289313122 Ack=0 win=5840		· <mark>(</mark>	
		192.168.0.99	192.168.0.9	TCP	32771 > 35174 [RST. ACK] Seg=0 Ack=289313123 win			
		192.168.0.9	192.168.0.99	TCP	35175 > 2005 [SYN] seq=291545065 Ack=0 win=5840			
		192.168.0.99 192.168.0.9	192.168.0.9 192.168.0.99	TCP	2005 > 35175 [RST, ACK] Seq=0 Ack=291545066 Win= 35176 > 437 [SYN] Seq=300016047 Ack=0 Win=5840 Li	0		
		192.168.0.99	192.168.0.9	TCP	437 > 35176 [RST, ACK] Seg=0 Ack=300016048 Win=0	er		
		192.168.0.9	192.168.0.99	TCP	35177 > 1544 [SYN] Seq=288811863 Ack=0 win=5840	Lf		
		192.168.0.99	192.168.0.9	TCP	1544 > 35177 [RST, ACK] Seq=0 Ack=288811864 win=)	
		192.168.0.9	192.168.0.99	TCP	35178 > 216 [SYN] Seq=288951110 Ack=0 Win=5840 L		/	
155566	1503.366368	192.168.0.99	192.168.0.9	TCP	216 > 35178 [RST, ACK] Seq=0 Ack=288951111 win=0	1.7		
F1						7		
E Frame	155545 (74	bytes on wire, 74 by	<pre>/tes captured) Dst: 00:60:08:a8:61:2</pre>			4		
E Inter	net Protocol	. Src Addr: 192.168	0.9 (192.168.0.9). Ds	4 1 Addr: 192	.168.0.99 (192.168.0.99)			Drotocol dotoilo
⊞ Trans	mission cont	rol Protocol, Src P	ort: 35169 (35169), Ds	t Port: dom	ain (53), Seq: 303023968, Ack: 0, Len: 0			Protocol details
Sec. Sec.						H		
RI						7 -	<u>_</u>	
00000 0	0 60 08 a8 6	1 24 00 10 a4 c5 7	c 38 08 00 45 00	.a\$ 8.		121		
0010 0	0 3c e3 b7 4 0 63 89 61 0	0 00 40 06 d5 47 c 0 35 12 0f c7 60 0		.@.@G				
0030 1		0 00 02 04 05 b4 0	4 02 08 0a 01 02d					
0040 2	4 07 00 00 0	0 00 01 03 03 00	5			7		Raw data
Filter:				/ Reset /	Apply File: Scan1.log	academic 1		
(hanness				and anomalia	and and a second se		2	

TCP connect scan

 Repeated TCP SYN requests to different ports

		• • • • • •		今交	1 2016	i i i i i i i i i i i i i i i i i i i	X														
0	Time		ource			Destir				Protoco											
		846656 1					168.0			TCP							q=0 A				
		46705 1					$168.0 \\ 168.0$			TCP			> dom > 35				S0302			Ach	
		46761 1					168.0			TCP							87624				
		46772 1					168.0			TCP							a=0 A				
		46853 1			1. Con		168.0		Section 1	D.P.	1000	51650	: dom	ainea	to N	Seg	30302	3969	Act	129820	15505
155551	0 1503.3	846895 1	92.168.	0.9		192.3	168.0	.99		TCP	3	5171	> 213	[SYN] Se	q=286	71170	4 Ack	=0 W	n=584	10 Le
		846910 1					168.0			TCP							q=0 A				
		346953 1					168.0			TCP							60303				
		346961 1					168.0			TCP							eq=0				
		347004 1 347012 1					168.0			TCP							03229 eq=0				
		347012 1					168.0 168.0			TCP	7.	517/	331/	3 [RS 71 [r	:, A ⊻N]	Sector 2	eq=0 89313	ACK=3	ck=0	wdn-	5840
		847066 1					168.0			TCP							Sed=0				
		347114 1					168.0			TCP							15450				
		347122 1					168.0			TCP	2	005 >	3517	5 ERS	T, A	CK] S	eq=0	Ack=2	9154	5066 N	vin=0
15556	0 1503.3	847172 1	92.168.	0.9		192.	168.0	.99		TCP	3	5176	> 437	[SYN] Se	q=300	01604	7 Ack	=0 W	in=584	10 L6
		347181 1					168.0			TCP							q=0 A				
		347227 1					168.0			TCP							88118				
		347236 1					168.0			TCP							eq=0				
		473 00 1 366314 1					168.0			TCP							Seq. 95111				
		366368 1					168.0			TCP							a=0 V				
13330	0 1303.	200309 T	92.100.	0.99		192.	108.0	. 9		ICP	٤.	TO >	33710	[K21	, AL	V] 26	q=0 A	CK = 20	1033T	LTT W	111=0
										1441											
		5 (74 by																			
Ether	net II,	Src: 0	0:10:a4	:c5:70	::38, D:	t: 00	:60:0	8:a8:	61:24												
Inter	net pro	tocol, Contro	Src Add	ir: 192	2.168.0.	9 (19	2.168	.0.9)	, DSt	Addr: 1	92.16	8.0.9	99 (19	2.168	1.0.9	9)					
ir and	511155101	1 Contro	Prote	, 2	SEC POPI	: 301	08 (3	PT0A)	, DSt	Port: d	omain	(53	, sec	1: 303	0239	108, 1	ACK: U), Ler	n: U		
000	00 60 01	8 a8 61	24 00 :	10 24	c5 7c	00 00	00.45			\$	0 5										
	00 3C A	3 b7 40	00 40	06 d5	47 c0 i					. G.											
020 0	00 63 8	9 61 00	35 12 1	of c7	60 00 1	00 00	00 a0	02	.c.a.	5											
		5 9b 00			b4 04 1	02 08	0a 01	. 02	ê												
040 3	24 d7 01	00 00 0	00 01 1	03 03	00				5												

Open ports reply
 with SYN/ACK

Closed ports reply with RST/ACK

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

No					
	Time	Source	Destination	Protocol	info
		192.168.0.1 192.168.0.254	192.168.0.99 192.168.0.99	TCP	35964 > sunrpc [FIN, PSH, URG] Seq=0 Ack=0 Win=30
		192.108.0.254	192.168.0.99	TCP	35964 > sunrpc [FIN, PSH, URG] Seq=0 Ack=0 win=30
		192.168.0.199		TCP	35964 > sunrpc [FIN, PSH, URG] Seg=0 Ack=0 win=30
161284	1644.943028	192.168.0.1	192.168.0.99	TCP	35964 > 597 [FIN, PSH, URG] Seg=0 Ack=0 win=3072
		192.168.0.254	192.168.0.99	TCP	35964 > 597 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
		192.168.0.9	192.168.0.99	TCP	35964 > 597 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
		192.168.0.99	192.168.0.9	TCP	597 > 35964 [RST, ACK] Seq=0 Ack=1 win=0 Len=0
		192.168.0.199	192.168.0.99	TCP	35964 > 597 [FIN, PSH, URG] Seq=0 Ack=0 w1n=3072 35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 w1n=3072
		192.168.0.254	192.168.0.99	TCP	35965 > 381 [FIN, PSH, URG] SEG=0 ACK=0 Win=3072 35965 > 381 [FIN, PSH, URG] SEG=0 ACK=0 Win=3072
161291	1645.252197	192.168.0.9	192.168.0.99	TCP	35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
161292	1645.252204	192.168.0.99	192.168.0.9	TCP	381 > 35965 [RST, ACK] Seg=0 Ack=1 win=0 Len=0
		192.168.0.199		TCP	35965 > 381 [FIN, PSH, URG] Seg=0 Ack=0 win=3072
161294	1645.252267	192.168.0.199 192.168.0.1 192.168.0.254	192.168.0.99 192.168.0.99 192.168.0.99	ТСР ТСР ТСР	35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
161294 161295	1645.252267 1645.252295	192.168.0.1 192.168.0.254	192.168.0.99 192.168.0.99	TCP	35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 win=3072 1 35965 > 1025 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
161294 161295	1645.252267 1645.252295 161282 (60	192.168.0.1 192.168.0.254	192.168.0.99 192.168.0.99 60 bytes captured)	ТСР ТСР	35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 win=3072 1 35965 > 1025 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
161294 161295 Frame : Ethern	1645.252267 1645.252295 161282 (60 et II, Src:	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8:	TCP TCP 61:24	35965 > 381 [FIN, PSH, URG] Seq=0 Ack-0 win=3072 35965 > 1025 [FIN, PSH, URG] Seq=0 Ack-0 win=3072 35965 > 1023 [FIN, PSH, URG] Seq=0 Ack-0 win=3072 1 ⊂
161294 161295 E Frame S E Ethern E Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	33965 > 381 (FIN, PSH, URG) Seq-0 Ack+0 Win=3072 33965 > 1025 (FIN, PSH, URG) Seq-0 Ack+0 Win=3072 33965 > 1025 (FIN, PSH, URG) Seq=0 Ack+0 Win=3072 20168,0,99 (192,168,0,99)
161294 161295 E Frame S E Ethern E Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	35965 > 381 [FIN, PSH, URG] Seq=0 Ack=0 win=3072 35965 > 1025 [FIN, PSH, URG] Seq=0 Ack=0 win=3072 35965 > 1023 [FIN, PSH, URG] Seq=0 Ack=0 win=3072
161294 161295 E Frame S E Ethern E Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	33965 > 381 (FIN, PSH, URG) Seq-0 Ack+0 Win=3072 33965 > 1025 (FIN, PSH, URG) Seq-0 Ack+0 Win=3072 33965 > 1025 (FIN, PSH, URG) Seq=0 Ack+0 Win=3072 20168,0,99 (192,168,0,99)
161294 161295 E Frame S E Ethern E Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	33965 > 381 (FIN, PSH, URG) Seq-0 Ack+0 win=3072 33965 > 1025 (FIN, PSH, URG) Seq-0 Ack+0 win=3072 33965 > 1025 (FIN, PSH, URG) Seq-0 Ack+0 win=3072 20168,0,99 (192,168,0,99)
161294 161295 Frame Ethern Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	33965 > 38L [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq=0 Ack+0 Win=3072 20168.0.99 (192.168.0.99)
161294 161295 Frame Ethern Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192	33965 > 38L [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq=0 Ack+0 Win=3072 20168.0.99 (192.168.0.99)
161294 161295 Frame Ethern Intern	1645.252267 1645.252295 161282 (60 et II, Src: et Protocol	192.168.0.1 192.168.0.254 bytes on wire, 00:10:a4:c5:7 , Src Addr: 19	192.168.0.99 192.168.0.99 60 bytes captured) c:38, Dst: 00:60:08:a8: 2.168.0.9 (192.168.0.9)	TCP TCP 61:24 , Dst Addr: 192 , Dst Port: sur	33965 > 38L [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq-0 Ack+0 Win=3072 33965 > 1025 [FIN, PSH, UKG] Seq=0 Ack+0 Win=3072 20168.0.99 (192.168.0.99)
161294 161295 I Frame : I Ethern I Intern I Transm	1645.25267 1645.252295 161282 (60 et II, Src: et Protocol 15s1on Cont	192.168.0.1 192.168.0.254 bytes on wfre, 00:10:a4:c5:7 , Src Addr: 19 rol Protocol,	192.168.0.99 192.168.0.99 60 bytes captured) c:38, 0st: 00:60:08:88 2.188.0.9 (192.168.0.9) Src Port: 35964 (35964)	TCP TCP 61:24 , Dst Addr: 192 , Dst Port: sur	35065 > 381 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35065 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35065 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 2.168.0.99 (192,168.0.99) mpc (111), Seq: 6, Ack: 0, Len: 0
161294 161295 B Frame : B Ethern B Intern B Transm 000 00 000 00	1645.25267 1645.252295 161282 (60 et II, Src: et Protocol 1ssion Cont	192.168.0.1 192.168.0.254 bytes on wire, 00:10:44:C5:7 .5rc Addr: 19 rol Protocol,	192.168.0.99 192.168.0.99 60 bytes captured) c:18.09t: 00:60:08:18 2.188.0.9 (192.168.0.9) Src Port: 35964 (35964) 5 c 7c 38 08 00 45 00 da c0 48 00 09 c0 a8	TCP TCP 61:24 , Dst Addr: 192 , Dst Port: sur	33965 > 381 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 2.166.0.99 (192.168.0.99) wpc (111), Seq: 0, Ack: 0, Len: 0
161294 161295 Frame : Ethern I Transm 000 00 010 00 020 00	1645.252267 1645.252295 161282 (60 et II, Srcc) et Protocol 15s1on Cont 15s1on Cont	192.168.0.1 192.168.0.254 bytes on wire, 00:10:44:C5:7 , Src Addr: 19 rol Protocol, 124 00 10 44 0 00 26 66 b3 06 70 00 00	192.168.0.99 192.188.0.99 60 bytes captured) c:38, 081: 00:60:08188 2.168.0.9 (302.168.0.9) Src Port: 35964 (35964) 5rc Port: 35964 (35964) (35 7C 38 08 00 45 00 (36 CC 38 08 00 45 00 (36 00 00 20 00 00 50 25	TCP TCP 61:24 , Dst Addr: 192 , Dst Port: sur	33965 > 381 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 2.166.0.99 (192.168.0.99) wpc (111), Seq: 0, Ack: 0, Len: 0
161294 161295 3 Frame 3 3 Ethern 3 Transm 000 00 010 00 020 00	1645.25267 1645.252295 161282 (60 et II, Src: et Protocol 1ssion Cont	192.168.0.1 192.168.0.254 bytes on wire, 00:10:44:C5:7 , Src Addr: 19 rol Protocol, 124 00 10 44 0 00 26 66 b3 06 70 00 00	192.168.0.99 192.168.0.99 60 bytes captured) c:18.09t: 00:60:08:18 2.188.0.9 (192.168.0.9) Src Port: 35964 (35964) 5 c 7c 38 08 00 45 00 da c0 48 00 09 c0 a8	TCP TCP 61:24 , Dst Addr: 192 , Dst Port: sur	33965 > 381 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 35965 > 1025 [FIN, PSH, URG] Seq-0 Ack-0 win-3072 2.166.0.99 (192.168.0.99) wpc (111), Seq: 0, Ack: 0, Len: 0

Open ports do not reply

Closed ports reply with RST/ACK

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

D B A X				
p . Time	Source	Destination	Protocol	Infa.
Ethernet II, S	<pre>8 192.168.1.200 7 192.168.1.1 8 192.168.1.1 1 192.168.1.1 1 192.168.1.200 1 192.168.1.200 1 192.168.1.200 1 192.168.1.200 1 192.168.1.200 1 192.168.1.200 1 192.168.1.200 1 192.168.1.1 9 192.168.1.200 1 1 192.168.1.200 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>	DST: 00:02:b3:06:5f: 3.1.1 (192.168.1.1), D	st Addr: 192	27774 7 1006 [071, ac] 502(443) 9754 Ac] 50475 2 1 27774 7 1006 [071, ac] 502(443) 9754 Ac] 50741 2 1 27774 7 1006 [071, ac] 502(443) 9754 Ac] 50741 2 1 27774 7 1006 [071, ac] 502(443) 9741 Ac] 50741 2 1 27774 7 1006 [071, ac] 502(443) 9741 Ac] 504761 1 27774 7 1006 [071, ac] 502(443) 9741 Ac] 5475761 1 27774 7 1006 [071, ac] 502(443) 9761 Ac] 544519761 1 27774 7 1006 [071, ac] 562(443) 9761 Ac] 544519761 1 27774 7 1006 [071, ac] 562(443) 9761 Ac] 544519761 1 27774 7 1006 [071, ac] 562(443) 9761 Ac] 544519761 1 27774 7 1006 [071, ac] 562(443) 9761 Ac] 544519761 1 27774 7 1006 [071, ac] 562(443) 9761 Ac] 544519761 1 1008 2 7777 [Ac] 562(443) 9761 Ac] 54451978 Ac] 544451978 1 1008 2 7777 [Ac] 562(443) 98701 Ac] 54451978 Ac] 544451978 Ac] 54451978
	6 5f 5a 00 03 47 8b d 40 00 80 06 00 00	c0 a8 01 01 c0 a8 .0		

Many TCP packets through port 27374

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

<pre>[connected: 14:41 - November 7, 2003, Friday, ver: Legends 2.1RSHC:RSH03409ancldr.exe0 Aurosetup.exe0 Aurosety.exe0 commeads.dbg0 commeads.dbg0 commed: 0bg1 CowLittings.log0 cowLittings.ad Settings>0 coRLittings.ad Settings>0 coRLittings.ad Settings>0 coRLittings.ad Settings>0 coRLittings.ad Settings>0 coRLittings.ad Settings>0 corrections.ad Settings corrections.ad Settings corrections</pre>	٥
ncldr0 <oracle>0 pagefile.sys0 <program files="">0 <recyclen0< th=""><th></th></recyclen0<></program></oracle>	
<samplesite>D secret.txtD <snort>D</snort></samplesite>	
<pre>cSystem volume Information>U <comppl <ul="" <unrightarrowsel=""> <unrightarrowsel <="" <unrightarrowsel="" ul=""> </unrightarrowsel></comppl></pre>	a#

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

TC/BUPT/8-7-04

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

@ Scan3.log - Ethereal			
File Edit View Capture Analyze Help			
	DBXD		
No Time Source	Destination	Protocol	Info
33 15061, 54864 68, 37, 54, 69	172.10.134.120	DEERRE	Ping: seq_num: 16845009
45 22326.71619 12.252.61.161	172.16.134.191	DCERPC	Ping: seq_num: 16843009
104 51561.94488 206.149.148.192	172.16.134.191	SEBEK	SEBEK - pid(16843009) uid(16843009) fd(16843009)
148 81237.81969 218.4.87.137	172.16.134.191	DCERPC	Ping: seq_num: 16843009
149 82141.42831 66.81.131.17 152 89544.06919 61.177.56.98	172.16.134.191 172.16.134.191	DCERPC	Ping: seq_num: 16843009 Ping: seq_num: 16843009
191 105791.7621 61.132.88.90	172.16.134.191	DCERPC	Ping: seq_num: 16843009
192 106708.6318 24.167.221.106	172.16.134.191	DCERPC	Ping: seq_num: 16843009
244 134238.8786 67.201.75.38	172.16.134.191	DCERPC	Ping: seq_num: 16843009
245 145180.7410 61.8.1.64	172.16.134.191	DCERPC	Ping: seg_num: 16843009
248 152927, 4822 61, 132, 88, 90	172.16.134.191	DCERPC	Ping: seg_num: 16843009
260 159581.5442 68.84.210.227	172.16.134.191	DCERPC	Ping: seg_num: 16843009
261 160035.4086 66.233.4.225	172.16.134.191	DCERPC	Ping: seq_num: 16843009
271 163796.8138 200.50.124.2	172.16.134.191	DCERPC	Ping: seq_num: 16843009
272 234065.2600 12.253.142.87	172.16.134.191	DCERPC	Ping: seq_num: 16843009
	2 2 / 2 2 /2		1.0010000
∃ Frame 33 (418 bytes on wire, 418 byt	a charting and	3/3/3/2	15
BEthernet II, Src: 00:e0:b6:05:ce:0a,		2	
Binternet Protocol, Src Addr: 68.37.5			16 134 191 (172 16 134 191)
Source port: 1034 (1034)			
Destination port: ms-sql-m (1434)			
Length: 384			
Checksum: 0x8dac (incorrect, shou	d be 0x8407)		
B DCE RPC			
1000 01 31 CA 01 19 30 55 10 33 01 0	1 01 03 30 89 83 .1		
1000 01 31 C9 01 18 30 22 10 33 01 0 10C0 51 68 2e 64 6c 6c 68 65 6c 33 3	2 68 6b 65 72 6e Qh	dllhe 132hk	
0d0 51 68 6f 75 6e 74 68 69 63 6b 4	3 68 47 65 74 54 Qh	ounthi ckChG	etT
0e0 66 b9 6c 6c 51 68 33 32 2e 64 6	8 77 73 32 5f 66 f.	11qh32 . dhws	
0f0 b9 65 74 51 68 73 6f 63 6b 66 b 100 65 6e 64 be 18 10 ae 42 8d 45 d		Qhsoc kf.to	
0100 65 6e 64 be 18 10 ae 42 8d 45 d 0110 45 e0 50 8d 45 f0 50 ff 16 50 b		D.E.PP	
120 1e 8b 03 3d 55 8b ec 51 74 05 b	e 1c 10 ae 42 ff	=UQ T	
130 16 ff d0 31 c9 51 51 50 81 f1 0 140 01 01 01 01 51 8d 45 cc 50 8b 4	3 01 04 9b 81 f1	1.QQP	··· ,
140 01 01 01 01 51 8d 45 cc 50 8b 4	5 c0 50 ff 16 6a	Q.E. P.E.P	···] //
itter udp.dstport==1434	/ Day	Analy Steer	Datagram Protocol (udp), 8 bytes

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