

Surviving a Network Attack

Ron Trunk, CCIE, CISSP
Sr. Consultant
Chesapeake NetCraftsmen

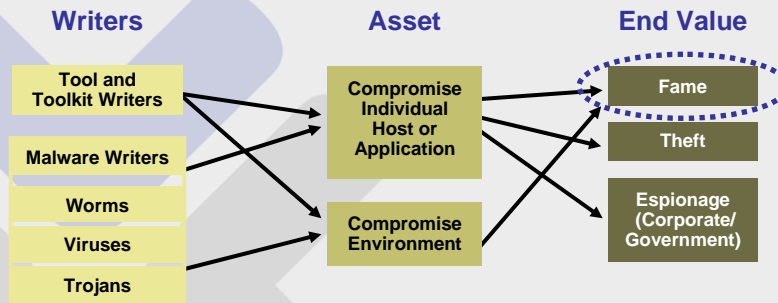
Agenda

- **What Are We Up Against?**
 - Understanding Recent Network Attacks
- **Building a Security Monitoring Infrastructure**
- **Practical Security Monitoring Techniques**

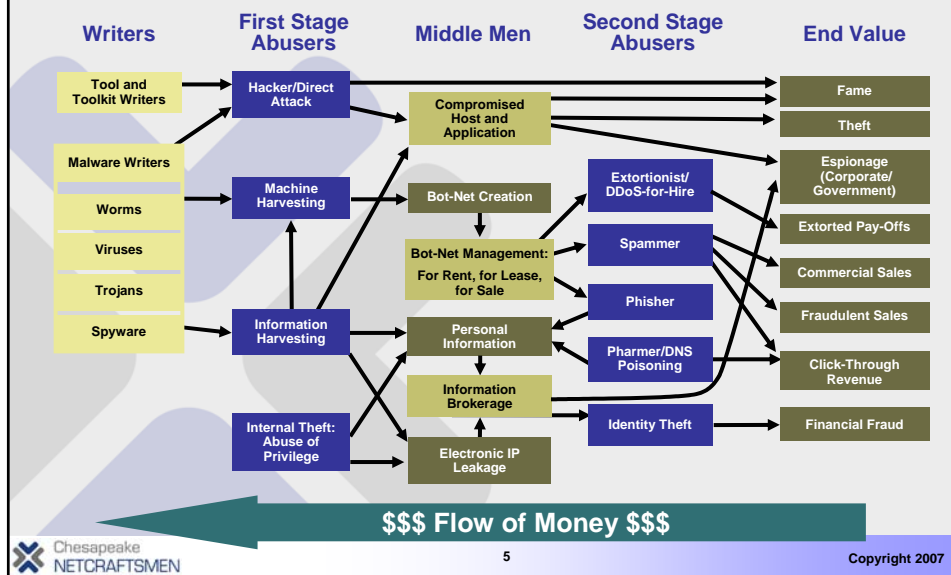
How Have Network Attacks Changed?

- No longer hackers out for glory
 - Real crime, financially motivated
 - FBI reports that in 2005, revenue from computer fraud exceeded revenue from drug trafficking
 - Real state-sponsored espionage
 - The Naval Network Warfare Command says Chinese hackers are relentlessly targeting Defense Department networks with cyber attacks. The "volume, proficiency and sophistication" of the attacks supports the theory that the attacks are government supported. The "motives [of the attacks emanating from China] ... include technology theft, intelligence gathering, exfiltration, research on DOD operations and the creation of dormant presences in DOD network for future action."
- Source <http://www.fcw.com/article97658-02-13-07-Web&printLayout>

Cybercrime Industry: In the Past



Cybercrime Industry : Today



The Cybercrime Industry

- Programming teams develop custom malware
- Custom malware is made available for purchase
- ISP administrators are paid to host malicious code on sites that they control
- Hosting services are for sale as part of the total package
- Credit card numbers and usernames and passwords are for sale
- Standard rates for data sales are being established

The Motivation Is Money

- Then:
- “Let’s break into the school’s network to alter a grade”
- Now:
- “Let’s steal a social security number that can earn me \$42 every time I sell it.”

How Much Money Do They Make?

- **Blue Security**, a security company that took on spammers aggressively, underwent a Distributed Denial of Service (DDoS) attack from zombie computers under control of a Russian speaking spammer.
- This spammer (or spam gang), which was called PharmaMaster, claimed to make \$3M dollars a month off of spam.
- Unwilling to give up that income, he paid a hacker \$2,000 an hour to perform the DDoS against Blue Security, its customers and its ISP.
- It cost him over \$1M dollars by the time all was said and done
- It exhausted the funding of Blue Security and they were forced to close shop.

Cyber Warfare

- “China is actively engaging in cyber reconnaissance by probing the computer networks of U.S. government agencies as well as private companies.
- The data collected from these computer reconnaissance campaigns can be used for myriad purposes, including identifying weak points in the networks, understanding how leaders in the United States think, discovering the communication patterns of American government agencies and private companies, and attaining valuable information stored throughout the networks. “
 - USSTRATCOM Commander General Cartwright in testimony before Congress, June 1, 2007

Increasing Malware Sophistication

- Teams of developers, just like legitimate developers
- Using all the modern tools
- Modular code written by specialists.
- Customizable for specific victims
- Increasing use of Zero-day attacks
- Botnets for rent

Malware Sophistication (con't)

- Hidden processes run in computer memory waiting to re-install the malware should some program remove it.
- Rootkits make the discovery of installed malware virtually impossible.
- Polymorphic code renders signature-based detection useless.
- Once a computer becomes compromised; it is likely to stay compromised.
- This leads to a growing number of flexibly updatable compromised computers on the Internet and in organization's internal network.

The Changing Nature of Network Attacks

- Increased targeted attacks
 - Attacks customized against specific targets, and occasionally people
 - Will your CEO click on a web link?
- Examples of attacks
 - Theft of data
 - Misuse of resources
 - Theft of intellectual property
 - Fraud against users
 - Extortion

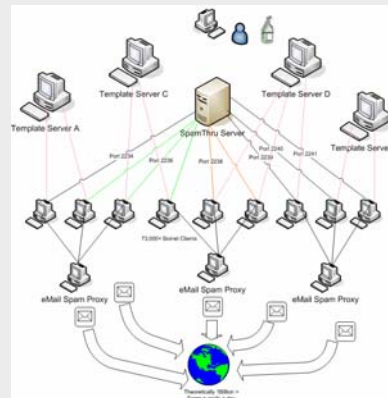
TJ MAXX

- **Biggest credit card number heist in history**
- Data harvesting started July 2005 and carried on through Dec. 2006
- Several banks and banking organizations sued TJX for not protecting customer data with “adequate security measures”
- 45.6M credit card numbers compromised



The Rise of Botnets

- **Attackers concentrate on clients, rather than servers**
- **Bots are rented out to**
 - Spammers
 - Phishers
 - Pump and dump stocks
 - Those guys sellingum....male enhancement supplements



Botnet Sophistication

- **Sophisticated command and control**
 - P2p and other techniques make it highly resilient
- **Bots have defensive capabilities**
 - Disable antivirus
 - Anti-debugging
 - Obfuscation
- **Botnet operators steal other botnets**
 - Forces developers to improve their code
 - Bots DoS other botnets
 - You're just collateral damage

Top 5 Reasons Why I think I'm Safe

1. There's nothing important on my computer
2. My A/V program said I didn't have a virus
3. I checked and I didn't see anything
4. My Corporate firewall will protect me
5. I have a Mac/Unix computer. They don't get viruses

5. I have a Mac/Unix computer.

McAfee lists 150 known attacks on MAC OS



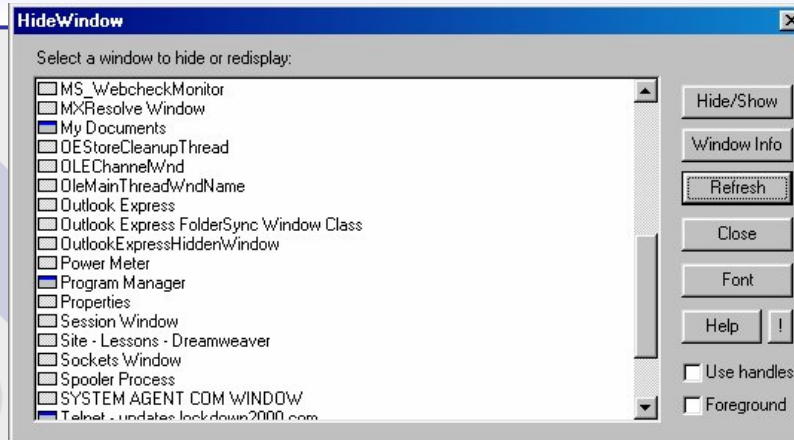
#1 platform for botnet command and control servers -
- UNIX



4. My Firewall Will Protect Me

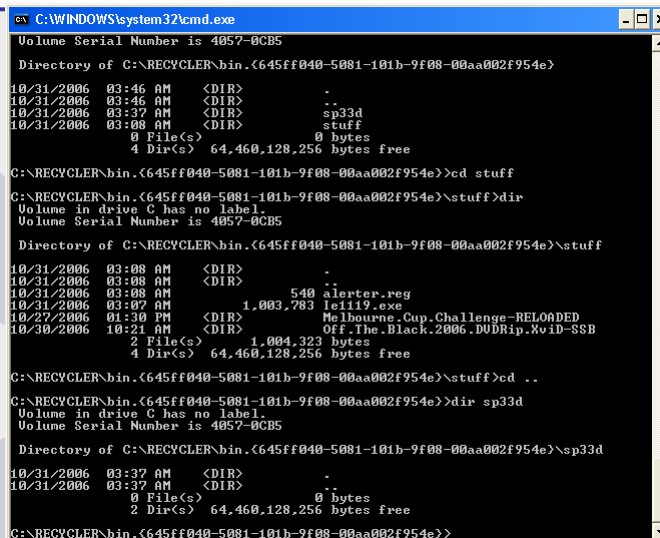
- Gartner estimates that more than 98% of organizations have an Internet firewall
- Yet network attacks are at an all-time high
- (Draw your own conclusion)
- Firewalls are simply not enough
 - Most attacks are user-pulled
 - Click on this link
 - Surf to bad page
- 10% of all web pages on the Internet have malware – Google

3. I checked and I didn't see anything



Hidden32.exe permits applications to run without using their GUI
HideUser2.exe adds an invisible user to the administrator group
User Mode rootkits
Kernel mode rootkits

3. I checked and I didn't see anything



2. A/V Program Said No Virus

```
net stop "Symantec antivirus client"
net stop "Symantec AntiVirus"
net stop "Trend NT Realtime Service"
net stop "Symantec AntiVirus"
net stop "Norton antivirus client"
net stop "Norton antivirus"
net stop "etrust antivirus"
```

Some bots leave the A/V tray icon and have a fake GUI!

2. A/V Program Said No Virus

Complete scanning result of "159130.ex_...", received in VirusTotal at 10.11.2006, 19:46:07 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntVir	7.2.0.25	10.11.2006	TR/Hijack.Site.6
Authentium	4.93.8	10.11.2006	no virus found
Avast	4.7.892.0	10.11.2006	Win32/Trojan-gen. (UPX)
AVG	386	10.11.2006	BackDoor.Generic3.HUD
BitDefender	7.2	10.11.2006	DeepScan.Generic.Malware.SMQw.85B75A93
CAT-QuickHeal	8.00	10.11.2006	no virus found
ClamAV	devel-20060426	10.11.2006	no virus found
DrWeb	4.33	10.11.2006	Trojan.SpamBot
eTrust-InoculateIT	23.73.19	10.11.2006	no virus found
eTrust-Vet	30.3.3127	10.11.2006	no virus found
Ewido	4.0	10.11.2006	Proxy.Small
Fortinet	2.82.0.0	10.11.2006	W32/Agent.DLEltr
F-Prot	3.16f	10.11.2006	no virus found
F-Prot4	4.2.1.29	10.11.2006	no virus found
IKarus	0.2.65.0	10.11.2006	no virus found
Kaspersky	4.0.2.24	10.11.2006	no virus found
McAfee	4871	10.11.2006	Generic BackDoor.I
Microsoft	1.1603	10.11.2006	no virus found
NOD32v2	1.1797	10.10.2006	a variant of Win32/Agent.NBE
Norman	5.80.02	10.11.2006	W32/Smalldoor.GME
Panda	9.0.0.4	10.11.2006	Adware/Popuper
Sophos	4.10.0	10.05.2006	no virus found
TheHacker	6.0.1.096	10.11.2006	Trojan.Generic
UNA	1.83	10.11.2006	no virus found
VBA32	3.11.1	10.11.2006	Trojan.SpamBot
VirusBuster	4.3.7.9	10.11.2006	no virus found

Additional Information

File size: 80896 bytes
MD5: 1a74375e5b7db6a92868d39c6deb3f66
SHA1: 806affca800728d538e8e9e927bb4eba62be35ee
packers: UPX
packers: UPX
packers: UPX

VirusTotal is a free service offered by [Hispasec, Sistemas](#). There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, these results DO NOT guarantee the harmlessness of a file. Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and malware.

1. Nothing Important

Your space, network, & processing power

- Child Pornography
- SPAM
- Stolen movies, games, & software

Your access

- Bank Accounts
- SSN
- Work accounts
- Your email

Your money

Your identity

A Recent Attack: The Storm Worm

- **Old classification schemes don't work**
 - Is it a Virus? Worm? Trojan, Backdoor?
- **First noticed January 2007**
 - At its peak, more than a million PC infected
 - 80% on ATT and SBC Global networks
 - Currently more than 50,000
 - Microsoft MSRT responsible for a lot of clean up.
- **Usually a attachment to email, enticing you to run attachment, or click on link.**
 - Note: It's not just clueless users. Everybody can be fooled.
- **Infected machines used mostly for spamming**
- **Downloads any number of trojans, allowing remote control of computer.**

Storm Update (Nov 14)

- Storm-controlled bots are now sending spam with links to GeoCities sites.
- Those sites have been seeded with malicious code to redirect browsers to other URLs that attempt to manipulate users into downloading a codec advertised as being necessary for viewing GeoCities site images;
- it is actually malware designed to steal sensitive data.
- This attack is also believed to have connections to RBN.

What makes Storm Notable?

- Uses peer-to-peer networking for command and control. No central command site to disrupt.
- New payloads being created faster than antivirus can detect them.
 - Antivirus detects payload, just download another one.
- Command sites counter attack (DoS Flood) if probed.
- Storm will probably never be eradicated

The Bottom Line

- **Worms, Viruses and Malware are here to stay**
- **They will increase in capabilities, stealth and sophistication**
- **You will always face unknown, unexpected attacks**
- **You won't be able to prevent attacks.**
- **But you can**
 - Minimize their impact
 - Reduce your losses
 - React more rapidly
 - Block, disable or repair more quickly

Agenda

- **What Are We Up Against?**
 - Understanding Recent Network Attacks
- **Building a Security Monitoring Infrastructure**
- **Practical Security Monitoring Techniques**

Building a Security Monitoring Infrastructure

- A collection of tools and agents that will provide you with actionable network events
- Related to network performance monitoring, but different focus
- Related to capacity planning, but with different focus.

What Does Monitoring Do For Me?

- Detects attacks
- Provides information for deeper analysis
 - Who?
 - Where?
 - When?
 - How many?
- Allows trend analysis and event correlation
- Informs corrective action

Where Does Data Come From?

- **Syslog**
 - Firewall Logs
 - Router and Switch Logs
 - Unix Syslogs
 - Windows Events
- **NetFlow**
- **Packet Capture (sniffing)**
- **IDS/IPS sensors**

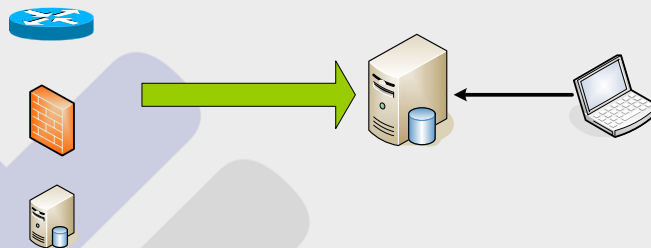
Where Does The Data Go?

- **Tools to Collect, Analyze and Report on Network Security Data**
 - Snort
 - Syslog-NG
 - Sawmill
 - Cisco IDS/IPS
 - CS-MARS
 - OSU Flow Tools
 - NetQoS
- **Your choice: commercial products or open source**
 - Many, many good Unix tools
 - Commercial tools good, but more expensive

Syslog

- **Syslog server is a central repository for system messages**
- **All Unix/Linux systems have it built-in**
- **Many free Windows tools**
 - Kiwi Catools
 - 3cDaemon
 - Others
- **For Unix, syslog-ng (next generation) is an enhancement to the standard daemon**
 - Segregate data by source, type, severity, date, etc.
- **For Windows, use SNARE to write windows events to a syslog server**

Syslog



- **Syslog uses UDP port 514**
 - Unreliable transport
- **Can also use TCP port 1468**
 - Reliable transport
 - Not all devices support this

Configuring Syslog on IOS

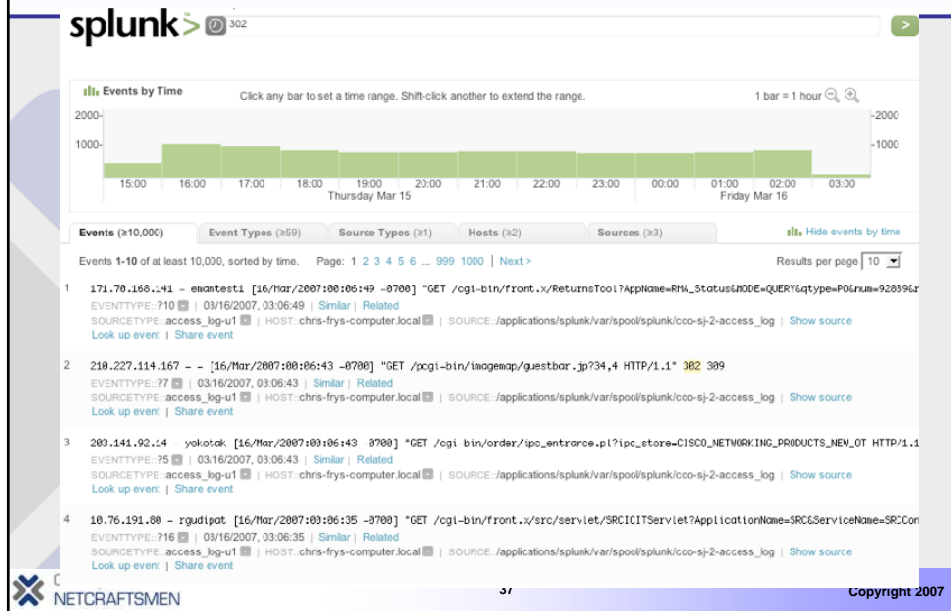
- `MyRouter(config)# logging on`
- `MyRouter(config)# logging 172.36.7.5`
- `MyRouter(config)# logging source-interface Loopback0`
- `MyRouter(config)# end`
- `MyRouter#`

Logging has Performance Impact

- **Router Access Control List (ACL) logs**
 - High event volumes
 - Can impact performance
 - Rate-limiting possible
- **Pix and FWSM logs**
 - Also generate ACL logs
 - Performance impact much less than on routers
- **OS and Application Logs**
 - Syslog, messages, authlog, access_log, etc.



Searching Through Logs w/Splunk



Searching Through Logs w/Sawmill


Sawmill Lite [Trial, 30 days left] Profile: test Logged in as 'cfry' Admin Logout Help About

Calendar Date Range Printer Friendly Update Database Rebuild Database

Individual sessions Row Numbers Zoom Options Export Table Options

Row 1 - 10 of 24,556 11-20 > >>> Start row: 1 Number of rows: 10

Session ID	User	Events	Start Time	End Time
1 192.63.136.118-2007-03-15 12:25:57	192.63.136.118	122 0.2 %	15Mar/2007 12:25:57	15Mar/2007 14:00:12
2 192.63.136.118-2007-03-15 09:28:50	192.63.136.118	100 0.1 %	15Mar/2007 09:28:50	15Mar/2007 10:29:51
3 71.168.213.78-2007-03-15 16:02:31	71.168.213.78	98 0.1 %	15Mar/2007 16:02:31	15Mar/2007 17:28:21
4 203.197.142.1-2007-03-15 22:06:34	203.197.142.1	92 0.1 %	15Mar/2007 22:06:34	16Mar/2007 00:05:38
5 209.47.179.250-2007-03-15 05:05:06	209.47.179.250	88 0.1 %	15Mar/2007 05:05:06	15Mar/2007 06:40:45
6 152.102.1.107-2007-03-15 00:13:01	152.102.1.107	80 0.1 %	15Mar/2007 00:13:01	15Mar/2007 01:04:54
7 166.42.249.221-2007-03-15 10:13:12	166.42.249.221	79 0.1 %	15Mar/2007 10:13:12	15Mar/2007 11:55:25
8 38.99.222.242-2007-03-15 09:55:43	38.99.222.242	75 0.1 %	15Mar/2007 09:55:43	15Mar/2007 11:06:18
9 208.214.139.134-2007-03-15 12:46:24	208.214.139.134	75 0.1 %	15Mar/2007 12:46:24	15Mar/2007 14:15:08

 NETCRAFTSMEN

Other Logs



- **Web server logs**
 - Can verify and elaborate attacks**
 - Use HTTP status codes to determine if IDS alert really worked
 - Can provide URL details during attack
 - Apache**
 - Send as syslog via httpd.conf setting
 - IIS**
 - Send as syslog via MonitorWare Agent
- **App server logs**
 - Find way to relay as syslog
 - Send via SNMP events
 - Pull via SQL queries
- **Oracle logs**
 - Pull logs from AUD\$ table via SQL

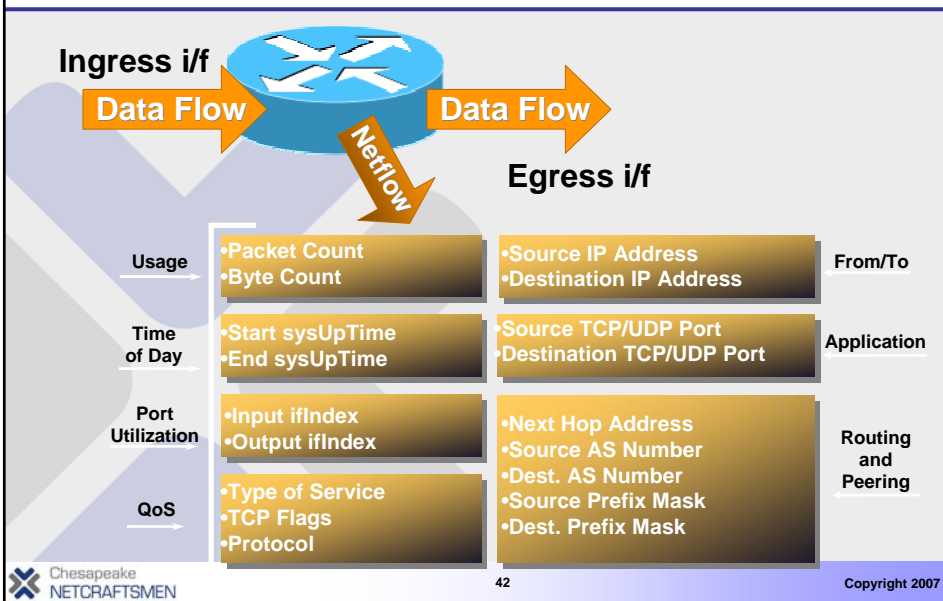
NetFlow

- **NetFlow is a form of telemetry pushed from the network devices.**
- **Describes traffic flows through the device**
- **Available on routers and larger switches**
- **If traffic capture is like a wiretap, NetFlow is like a phone bill**
 - **We can learn a lot from studying the network phone bill!**
 - Who's talking to whom? And when?
 - Over what protocols & ports?
 - How much data was transferred?
 - At what speed?
 - For what duration?

NetFlow

- Originally Cisco-proprietary, but soon to be standardized (v9) as Internet Protocol Flow Information Export (IPFIX)
- A “Flow” consists of at least five elements:
 - Source IP
 - Source Port
 - Dest IP
 - Dest Port
 - Protocol (tcp, udp)
- Netflow is best used in combination with other technologies: IPS, vulnerability scanners, and full traffic capture.

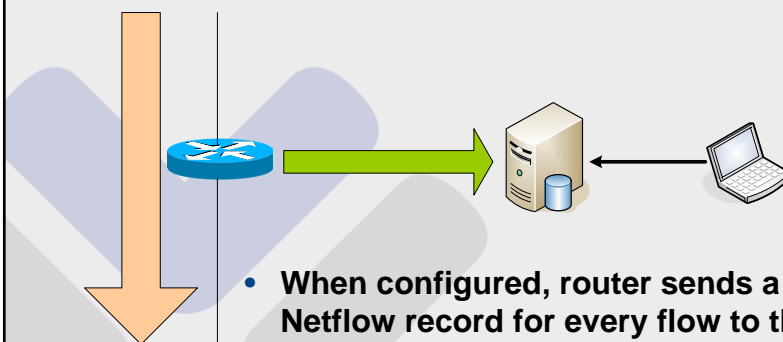
Elements of a Netflow Packet



Configuring Netflow on IOS

- `MyRouter(config)# ip flow-export version 5`
- `MyRouter(config)# ip flow-export destination 192.168.0.1 2055`
- `MyRouter(config)# ip flow-export source interface Loopback0`
- `MyRouter(config)# Interface FastEthernet 0/1`
- `MyRouter(config-int)# ip route-cache flow`
- `MyRouter(config-int)# end`
- `MyRouter#`

Netflow Data Collection



- When configured, router sends a Netflow record for every flow to the collector.
- Netflow collector stores Netflow records for later query and analysis

OSU Flowtools *Netflow Collector*

- Tool: OSU FlowTools
 - Free!
 - Developed by Ohio State University
- Examples of capabilities
 - Did **192.168.15.40** talk to **216.213.22.14**?
 - What hosts and ports did **192.168.15.40** talk to?
 - Who's connecting to port **TCP/6667**?
 - Did anyone transfer data > **500MB** to an external host?



OSU Flowtools Example *Who's Talking?*

- Scenario: New botnet, variant undetected

You need to identify all systems that 'talked' to the botnet Command & Control

Luckily you've deployed Netflow collection at all your PoPs

flow.acl file uses familiar ACL syntax. create a list named 'bot'

concatenate all files from Feb 12, 2007 then filter for src or dest of 'bot' acl

we've got a host in the botnet!

```
[myrfchost]$ head flow.acl
ip access-list standard bot permit host 69.50.180.3
ip access-list standard bot permit host 66.182.153.176

[myrfchost]$ flow-cat /var/local/flows/data/2007-02-12/ft* | flow-filter sbot -o
-...
```

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress
DstP						
0213.08:39:49.911	0213.08:40:34.519	58	10.10.71.100	8343	98	69.50.180.3
31337						
0213.08:40:33.590	0213.08:40:42.294	98	69.50.180.3	31337	58	10.10.71.100
83						

Custom NetFlow Report Generator

Query by IP

Netflow Report Generator
 click on any of the links above the forms for help, or visit the [FAQ](#).

Source IP: Source Port: Destination IP: Destination Port:

☐ Use File for Source ☐ Use File for Destination

Time: Report: Netbios Resolve: Uniq:

DNS Resolve:

Netflow Collector:

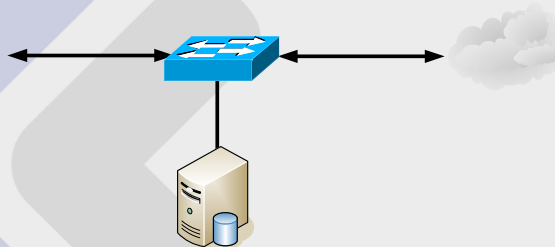
Email address:

DESTINATION:PORT	(HOSTNAME:DOMAIN:USER)	PACKETS	TIMESTAMP
60.190.22.153 [unknown]:7000		1	1205.21:35:59.
61.158.119.94 [unknown]:7000		1	1206.00:18:04.
61.152.107.59 [unknown]:7000		1	1206.00:23:00.
60.190.23.133 [unknown]:7000		1	1206.03:20:37.
61.152.107.59 [unknown]:7000		1	1206.11:15:55.
60.190.22.153 [unknown]:7000		1	1206.12:42:45.
60.190.23.153 [unknown]:7000		1	1206.12:58:27.

Chesapeake NETCRAFTSMEN 47 Copyright 2007

Full Packet Capture

- Capture and store every packet for later analysis
- No, I'm not crazy
 - Well, maybe a little bit, but that's between me and my therapist.



Full Packet Capture

- Not as difficult as you might imagine
- 1. Compute your average data rate
- 2. Multiply by storage time

- **Example: 5 day retention**

- 10Mb average rate
- 540GB of storage
- Less if compression used
- 1TB disks drives < \$350

Data Mb	GB
1	54
5	270
10	540
25	1,350
45	2,430
50	2,700
75	4,050
100	5,400

With Full Packet Capture You Can

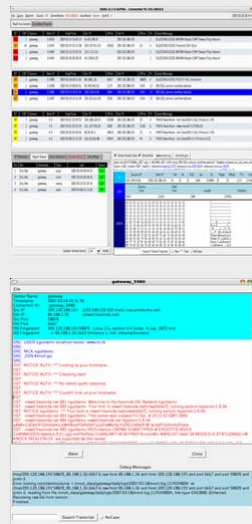
- **Analyze suspicious activity**
 - What did the user FTP to an external host?
- **Confirm alarms**
 - Was that really a Web attack?
- **Identify attack vectors**
 - Did host A download a trojan?
- **Provide evidence for legal action**
 - Capture complete conversation between hosts
- **Identify who talked to whom**
 - What other hosts did this host talk to?
- **Verify IDS or patch effectiveness**
 - After patching, replay attack. Did the patch work?

Full Packet Capture

- Capture data with
 - tethereal
 - tcpdump
 - Snort
- Snort can write directly to MySQL database
- Report using
 - any SQL reporting tool
 - Wireshark
 - Squil

Squil

- Analysis tool for packet capture
- Free! VM version available
- Query data
- Correlate with IDS alarms
- DNS lookups
- Ascii Dumps
- squil.sourceforge.net



Intrusion Detection / Prevention

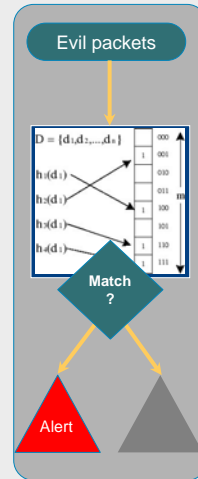
- **IDS - Intrusion Detection System**

passive network traffic monitoring
limited actions, mostly for alerting

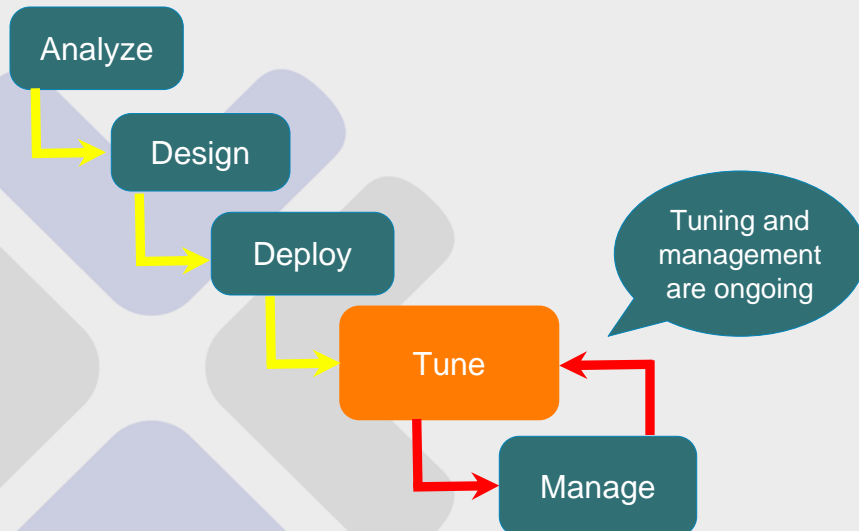


- **IPS - Intrusion Prevention System**

inline network traffic monitoring
alerting + ability to drop packets



IDS - Basic Deployment Steps



Tune IDS

- Use Cisco SAFE blueprint
- Critical to successful deployment
- Without tuning...
 - sensors generate alerts on **all** traffic matching criteria
 - alerts **overwhelm** monitoring staff
 - NIDS will produce events **irrelevant** to your environment
 - Will eventually cause NIDS to be **ignored** or disabled



Tune IDS



- Run in promiscuous mode
 - Default configuration
 - Latest signatures
- Tune out benign traffic using sensor
- Tune out benign traffic w/SIM (MARS, etc.)
 - Start with most frequent alerts
 - Trace to benign source/destination addresses
- Create location variables
 - Demarcations of your network (e.g. DNS, email, DMZ)
 - Elucidates traffic flows
 - Enables more targeted investigations
 - Allows tailoring of filters

Tune IDS Using Sensor

- Tune out benign traffic using sensor

```
xxx-dc-ids-1# show stat virt
Virtual Sensor Statistics
Statistics for Virtual Sensor vs0
<snip>
Per-Signature SigEvent count since reset
Sig 1101.0 = 22
Sig 3041.0 = 43
Sig 3052.0 = 1
Sig 3135.3 = 13
Sig 3159.0 = 12
Sig 5829.0 = 17
Sig 5837.0 = 22
Sig 5847.1 = 2
Sig 6005.0 = 281
Sig 6054.0 = 49
Sig 6055.0 = 7
Sig 3030.0 = 2045681
```

show statistics of the
virtual-sensor instance

**SigID 3030 is TCP
SYN host sweep,
need to look this one
up in MySDN**

Tune IDS Using CS-MARS

- Run reports of most frequent events over 24 hours
 - Start with the really noisy stuff
 - Tune at the IDS whenever possible
 - Get to where you're not affecting data retention with high volume false positives
 - On-going process: continually verify impact of new signatures
- Run reports to find high severity events over 24 hours
 - Verify alerts have appropriate severity level for your environment
 - Modify alert levels based on your policies & network topology
 - e.g. P2P coming from your datacenter should probably be higher than the default "Informational"

Time Synchronization



- Without it, can't correlate different sources
- Enable Network Time Protocol (NTP) everywhere supported by routers, switches, firewalls, hosts, and other network-attached devices
- Use UTC for time zones
- Any source is good enough
 - Synchronization is more important than accuracy

Agenda

- What Are We Up Against?
 - Understanding Recent Network Attacks
- Building a Security Monitoring Infrastructure
- Practical Security Monitoring Techniques

Recommendation: Best Monitoring Targets

1. Access sensitive data

- Legal compliance
- Intellectual property
- Customer sensitive data

2. Risky

Fewer controls (ACL's, poor configs, etc.)
Hard to patch (limited patch windows, high uptime requirements, custom vendor code, etc.)

3. Generate revenue

4. Produce actionable events

- Why monitor if you can't mitigate?

Monitor Policy Compliance

- Which policies to monitor?
 - Be concrete, precise
 - Which will management enforce?

- Policy types

Compliance with regulations or standards

SOX – monitor financial apps and databases
HIPAA – monitor healthcare apps and databases
ISO 17799 - best practices for information security

Employee policies

Rogue devices – laptops, wireless, DC devices, honeypots, etc.
Employees using shared accounts
Hardened DMZ devices – services running that should not be?
Direct login with privileged accounts (root, DBA, etc.)
Tunneled traffic – P2P, etc.

Example: COBIT DS9.4, Configuration Control

- Monitor changes to network devices, reconcile against approved change lists

Who changed the Pix config?

The screenshot displays a network security monitoring interface. At the top, a rule is defined: 'System Rule: Modify Network Config' with a status of 'Active'. Below this, a table lists incidents. The first incident, ID 12453563, is highlighted with an orange circle and a callout bubble asking 'Who changed the Pix config?'. The incident details show a 'PIX config written' event. The interface also includes a table for 'Incident ID: 12453563' with columns for Session / Incident ID, Event Type, Severity, Priority, Time, Reporting Device, Reported User, Path / Mitigate, and False Positive.

Offset	Open	Source IP	Destination IP	Service	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	1		

Offset	Session / Incident ID	Event Type	Severity	Priority	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1	S:11454408, I:12453563	PIX config written	0.0.0.0	0	172.16.0.1	0	N/A		False Positive
1	S:11454410, I:12453563	PIX end write config FAILED/OK	0.0.0.0	0	172.16.0.1	0	N/A		False Positive
1		Firewall begin config via reload or configure	172.16.4.60	0	172.16.0.1	0	N/A		Total: 2
1		PIX user entered a command that modified the config	0.0.0.0	0	0.0.0.0	0	N/A		Total: 2

Chesapeake NETCRAFTSMEN 63 Copyright 2007

Sample Policies to Monitor

- SSN's must be encrypted in storage (SB1386)
- Forbid copying data from production database to desktops
- Database cannot initiate connections outside data center
- No direct privileged logins to server or database
- Database must be hardened to the DISA Database STIG standard
 - No development in production
 - No developer logins in production
- Linux servers must be hardened to RedHat's recommended hardening.
 - No development in production
 - No developer logins in production

Example: FTP Root Login

```
evIdsAlert: eventId="1173129985693574851" severity="low" vendor="Cisco"
originator:
  hostId: rcdn4-dmz-nms-1
  appName: sensorApp
  appInstanceId: 421
time: Mar 22 2007 18:14:39 EDT (1174601679880242000) offset="0" timeZone="UTC"
signature: version="S31" description="Ftp Priviledged Login" id="3171"
  subsigId: 1
  sigDetails: USER administrator
  marsCategory: Info/Successful Login/FTP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 10.0.0.1 locality="OUT"
    port: 1387
  target:
    addr: 192.168.0.1 locality="IN"
    port: 21
    os: idSource="unknown" relevance="unknown" type="unknown"
summary: 2 final="true" initialAlert="1173129985693574773" summaryType="Regular"

alertDetails: Regular Summary: 2 events this interval ;
riskRatingValue: 37 targetValueRating="medium"
threatRatingValue: 37
interface: ge0_0
protocol: tcp
```

Caught
successful FTP
Administrator
login via IDS



Chesapeake
NETCRAFTSMEN

65

Example: SSH root login message

```
Mar 28 16:19:01 webserver1 sshd(pam_unix)[13698]:
session opened for user root by (uid=0)
```

Caught direct
root login via
syslog



Chesapeake
NETCRAFTSMEN

66

Copyright 2007

More Policy Monitoring Examples

- Policy: **No direct privileged logins**
Monitor IDS, SSH logs for successful *root* logins
- Policy: Use **strong passwords**
Vulnerability scan for routers with *cisco/cisco* credentials
- Policy: **No internet access from production servers**
Monitor for accepted connections to Internet initiated from servers
- Policy: **No protocol tunneling**
Monitor IDS alerts for protocols tunneled over DNS to/from non-DNS servers

Using Netflow

- Use a tool such as flow-dscan or nfdump to write an alert to syslog for file transfers sourced from the Oracle10g subnet

```
[myinfhost]$ head flow.acl  
ip access-list standard oracle10g permit 10.10.0.128 0.
```

flow.acl file uses
familiar ACL syntax.
create a list named
'oracle10g'

concatenate all files
from May 5, 2007,
filter for src of
'oracle10g' network,
write the results to
syslog

```
[myinfhost]$ flow-cat /var/local/flows/data/2007-05-05/ft* | flow-  
filter -Soracle10g | flow-dscan -O 50000000 | logger -f outputfile -  
p local4
```

```
[myinfhost]# crontab -e
```

```
* * * * * su - netflow -c "env LANG=C; DATE=`date +%Y"/"%m"/"%d`;  
flow-cat /var/local/flows/data/$DATE/ft* | flow-filter -Soracle10g |  
flow-dscan -O 500000000 | logger -f outputfile -p local4"
```

add the
command to
crontab for
automation

Custom Signature Example

- Use a custom signature to find cleartext instances of SSN's between any hosts except your Oracle10g web application servers

```
signatures 60001 0
!
sig-description
sig-name SSN_POLICY
sig-string-info SSN HANDLING POLICY VIOLATION
sig-comment CLEARTEXT SSN
exit
engine string-tcp
event-action produce-verbose-alert
specify-min-match-length no
regex-string ([0-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9][0-9][0-9])
service-ports 1-65535
exit
```

custom signature
60001
"SSN_POLICY"

regex to match SSN
format ###-##-####

Another Custom Signature

- Use a custom signature to find instances of the SQL "describe" command against production database

```
signatures 60002 0
!
sig-description
sig-name SQL_DESCRIBE
sig-string-info SQL dB enumeration
sig-comment Should not see in prod
exit
engine string-tcp
event-action produce-verbose-alert
specify-min-match-length no
regex-string [Dd][Ee][Ss][Cc][Rr][Ii][Bb][Ee]
service-ports 1433-1433
exit
```

Custom signature
60002
"SQL_describe"

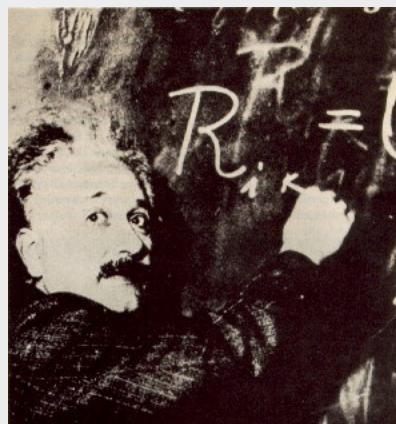
regex to match
SQL describe
command

Agenda

- **What Are We Up Against?**
 - Understanding Recent Network Attacks
- **Building a Security Monitoring Infrastructure**
- **Practical Security Monitoring Techniques**

In Summary

- **Network attacks will increase in sophistication and abilities.**
- **Start with tools you already have**
 - Syslog
 - Netflow
- **Add collection tools as time and budget permits**
- **Start small with IDS deployments**
 - Too many events at once is overwhelming



Summary (Con't)

- **Choose carefully what you want to monitor**
...or you'll waste your time chasing false positives
 - Understand "normal" traffic thoroughly before moving on
 - Avoid alerting on false-positives
 - Understand/tune each source before adding more
- **Select high value targets**
 - Mission Critical
 - Highly Visible
- **Use a correlation device (SIM) such as CS-MARS**
 - Event correlation, false positive reduction
- **Have allies in the IT support teams**
Network support, DBA's, webmasters, etc.
They can explain/remediate issues you find