TCPIP forensics

Share Session Anaheim

Laura Knapp
WW Business Consultant
Laurak@aesclever.com

Background

Incident Evaluation

Trace Evaluation

What is Computer Forensics

- Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Network or TCP/IP forensics involves the preservation, extraction, documentation and interpretation of TCP/IP data for evidentiary and/or root cause analysis
- Doesn't prevent computer crimes..after the fact investigation
- Forensics experts follow clear, well-defined mythologies and procedures

What is Network Forensics

- Network forensics entails monitoring network traffic and determining if there is an attack and if so, determine the nature of the attack
- Key tasks include traffic capture, analysis and visualization
- Network forensics systems can be one of two kinds:
  - *"Catch-it-as-you-can" systems*, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode
  - *"Stop, look and listen" systems*, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis

Employee Trust

•Construction Company

•Senior IT person also in charge of security
•Used cost issue to convince upper management to let him store data at his home rather than pay for external off-site storage
•Conflict arose between the Employee and Employer
•Employee sent email's to clients of the construction company indicating he had personal information
•Took 6 months to shut down the rogue employee after the employee used the internet to threatened people at which time the FBI became involved
•Construction company was fundamentally out of business

http://www.cio.com/article/454614/IT_Security_Pros_Share_Horror_Stories

Process Vulnerability

•Security administrator asked to shut off web security monitoring system as it was interfering with marketing's ability to access the corporate web site for creation and editing.
•Director said 'switch off' not….. find a work around…find a fix….just 'switch it off'
•Users quickly found that out that all web controls were no longer active
•A report surfaced that a user had used a desktop to access porn
•Due to the use of generic accounts tracking activity to a user was not possible
•Took 3 months, CCTV, internal and external police to finally catch the culprit
•To make matters worse the company dropped any further work on a security framework and made the security positions obsolete

itnews FOR AUSTRALIAN BUSINESS

KASPERSKY lab

News | Technology | Business | Forums

Reviews | Galleries | Events | Net Seminars | Whitepapers | Downloads | Newsl

Home > News > Technology > Security > Security experts beaten at their own game

SECURITY

Security experts beaten at their own ga

By Tom Sanders
Feb 9, 2007 1:36 PM
Tags: security | experts | beaten | own | game

RSA Conference delegates leave themselves wide open to attack.

More than half of the computers used by security experts attending the RSA Conference in San Francisco this week lack the proper protection and may have been compromised, according to wireless security firm AirDefense.

The company scanned all wireless traffic on the first day of the conference and found a total of 623 Wi-Fi enabled notebooks and mobile phones.

Some 56 per cent of these devices were configured automatically to log-on to networks with common names such as 'Linksys' or 'T-Mobile', a feature known as an open access wireless account.

Attackers could exploit the feature through a so-called man-in-the-middle

- RSA conference 2007
- Over half the computers lacked proper protection
  - Many configured to automatically log on to WiFI networks like ‘Linksys’ ‘T-Mobile’
- Five rogue networks mimicked common hotspot names
  - These could easily insert man in the middle routines and capture data
- The RSA conference had a SAFE WIFI network but it was toooooo complex to use and the help desk line was long and slow

2009 Litigation Highlights

Starwood v. Hilton (2009) - Complaint alleging that 2 former Starwood execs looted >100k Starwood computer files.

U.S. v. Chung (2009) – Boeing employee convicted at trial for passing trade secrets to Chinese government for 30 years. Co-defendant convicted and jailed for 24 years; Chung, 74 years old, received 15 years in prison.

-US v. Zhu (2009) – Indictment alleging Chinese national employed as engineer at US environmental company stole software from his employer and sold modified version to Chinese government.

US v. Lee (2009) – Former technical director of paint and coating company quit 2 weeks after return from business trip to China; discovered downloaded trade secrets, deleted files, one way ticket from Chicago to Shanghai.

Vistakon v. Bausch & Lomb (2009) – Subsidiary of J&J alleges that B&L misappropriated trade secrets in an effort to recruit sales force to bring new contact lens product to market quickly.

The Impact of a Digital Crime

- Disruption to organizational routines and processes
- Direct financial losses through information theft and fraud
- Decrease in shareholder value
- Loss of privacy
- Reputational damage causing brand devaluation
- Loss of confidence in IT
- Expenditure on information security assets and data damaged, stolen, corrupted or lost in incidents
- Loss of competitive advantage
- Reduced profitability
- Impaired growth due to inflexible infrastructure/system/application environments
- Injury or loss of life if safety-critical systems fail

- Theft of trade secrets exceeded $1 trillion in 2008 and continues to escalate
- Over 40% of U.S. businesses have reported intellectual property losses in 2008

Background

Incident Evaluation

Trace Evaluation

Incident Reporting

Law Enforcement report?

Regulatory agency report?

Insurance claim?

Disciplinary action?

Dismissal action?

Vendor report?

Update disaster recovery plan?

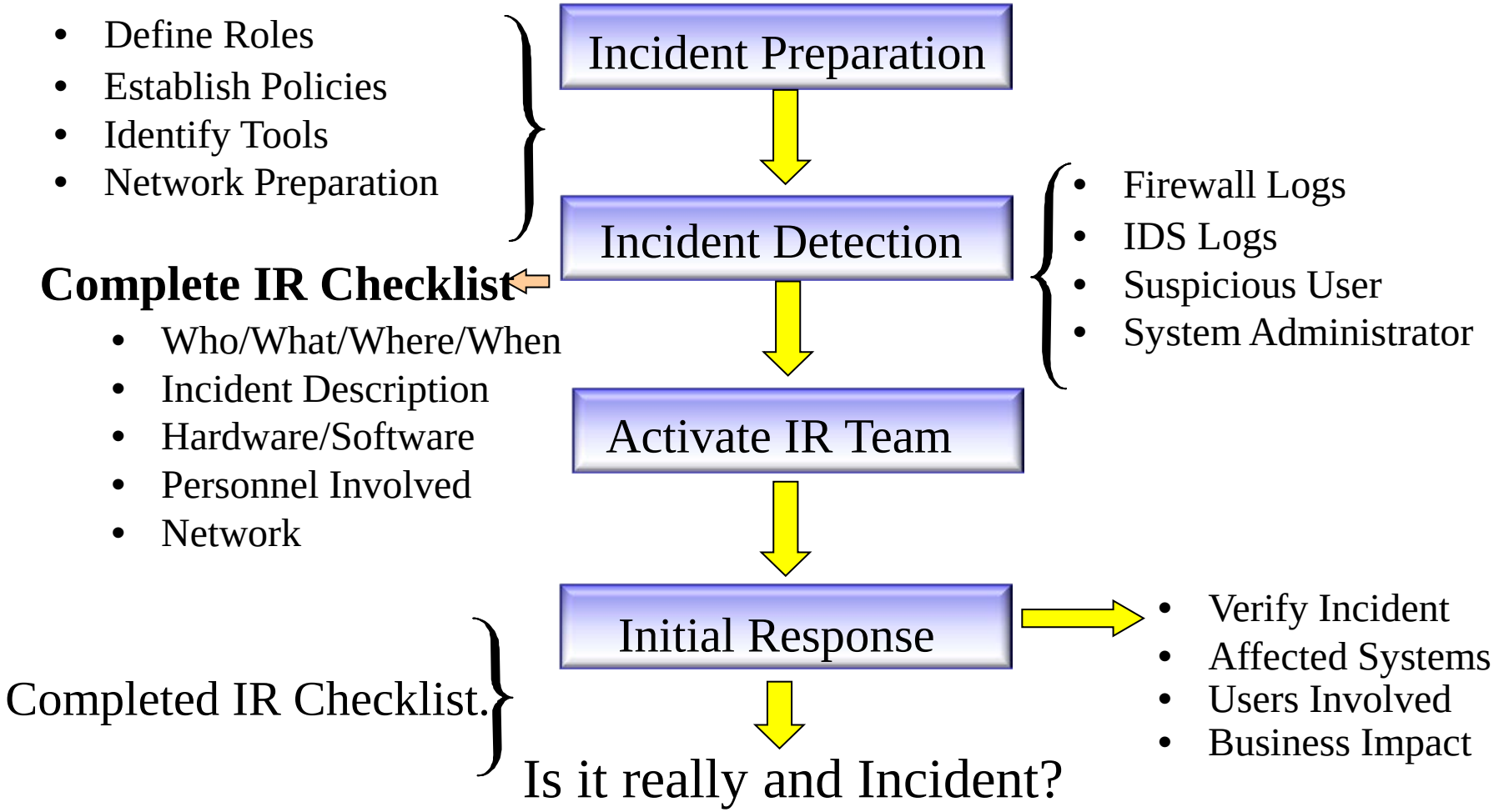
Update software to new versions?

Update employee training?

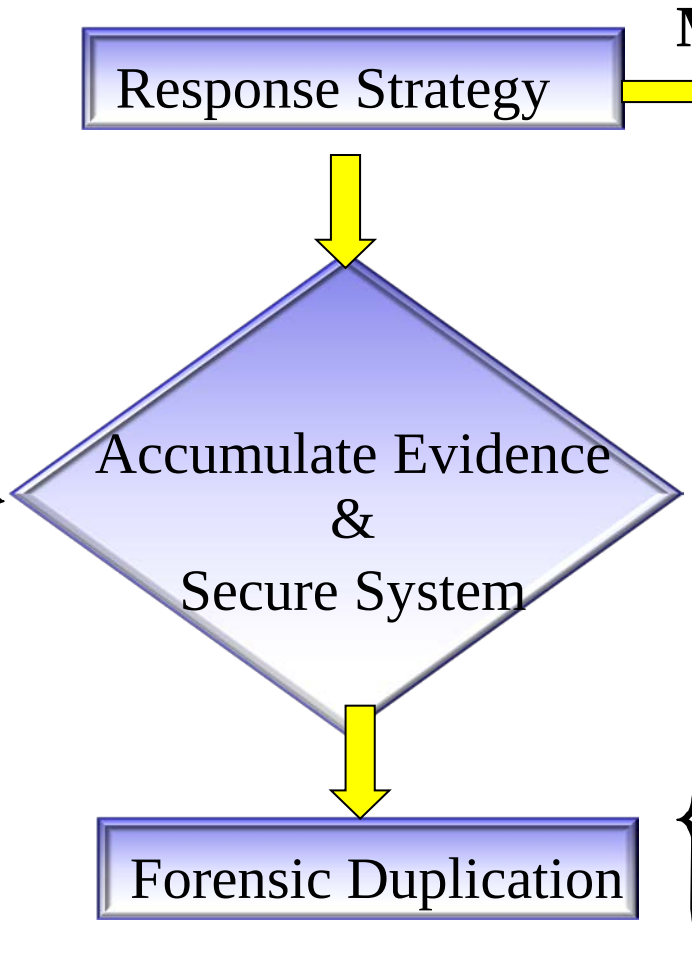
Public Affairs report?

CEO report to employees?

Incident Response Process



Incident Response Process Response



Management Approval

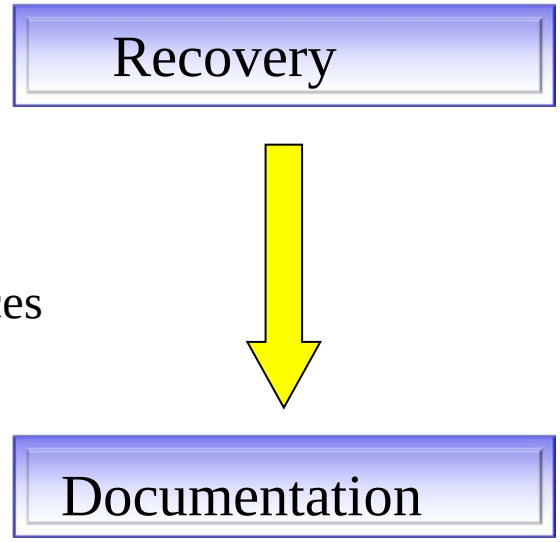
- Dollar Loss
- Downtime
- Legal Liability
- Publicity
- Intellectual Property

- System Criticality
- Information Sensitivity
- Perpetrators
- Publicity
- Skill of Attacker
- System Downtime
- Dollar Loss

- Best Evidence Rule
- Chain of custody
- Data Volatility

Incident Response Process Improvements

- New Procedures
- Reinstall files
- Reinstall from CD-Rom
- Secure System
  - Turnoff unneeded services
  - Apply patches
  - Strong Passwords
  - Strong Administration



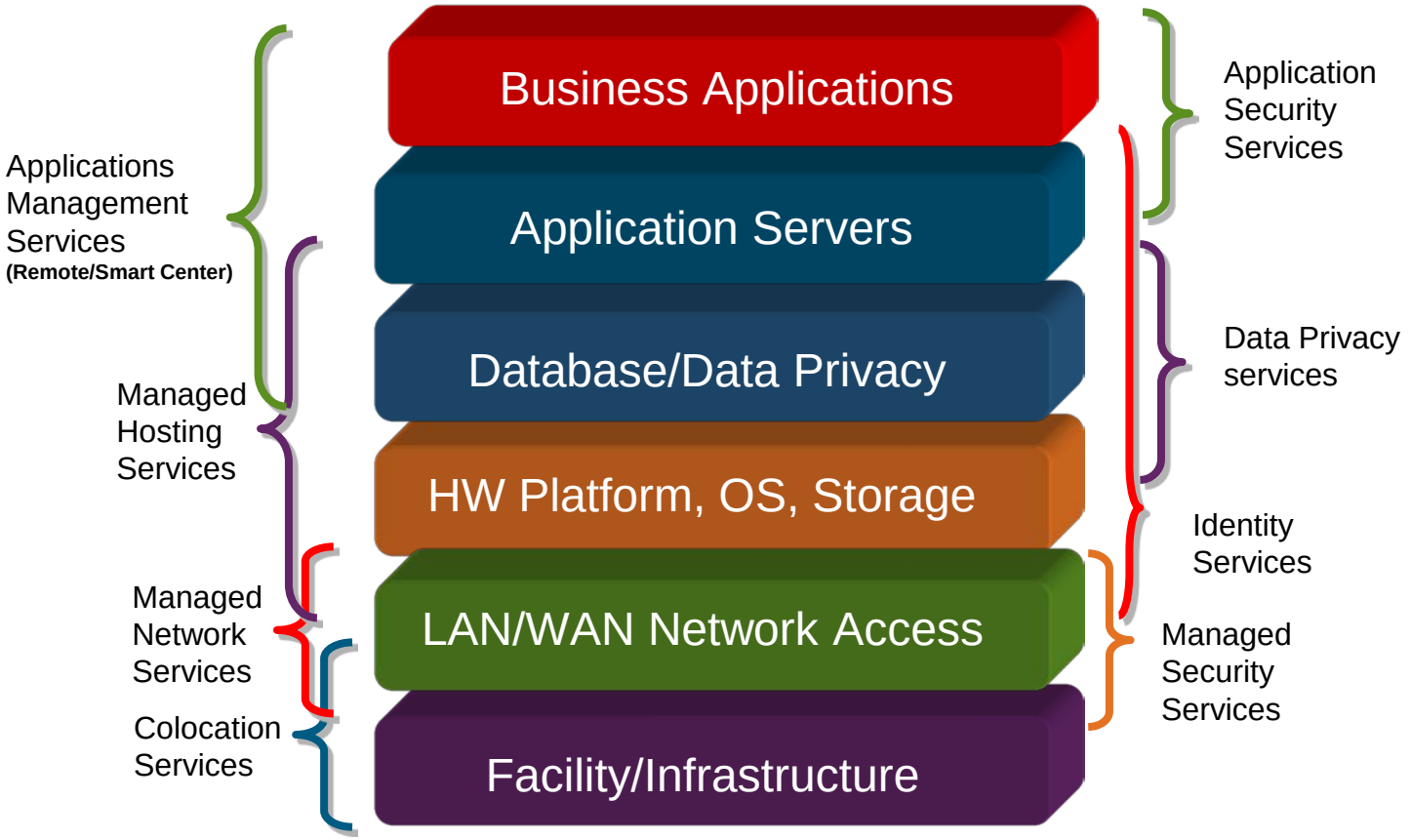
- Document everything as it occurs
- Support both criminal and civil prosecution
- Produce the final report
- Process improvement

Background

Incident Evaluation

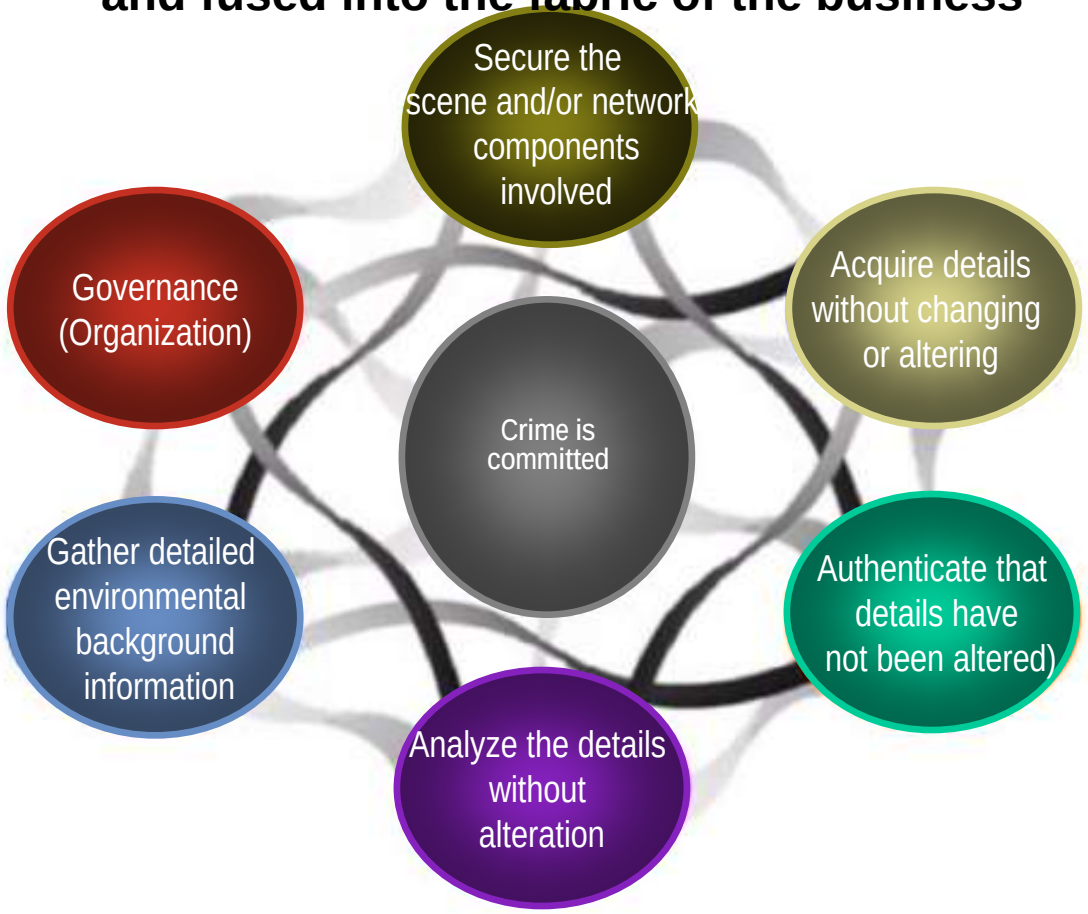
Trace Evaluation

Elements of Digital Forensics



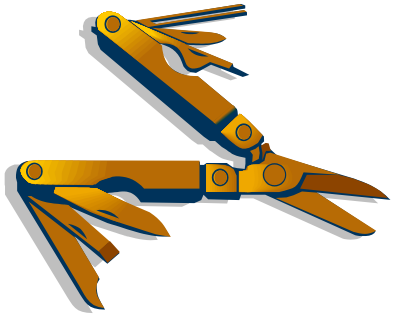
Network Forensics Elements

Security has to be applied within a business context and fused into the fabric of the business



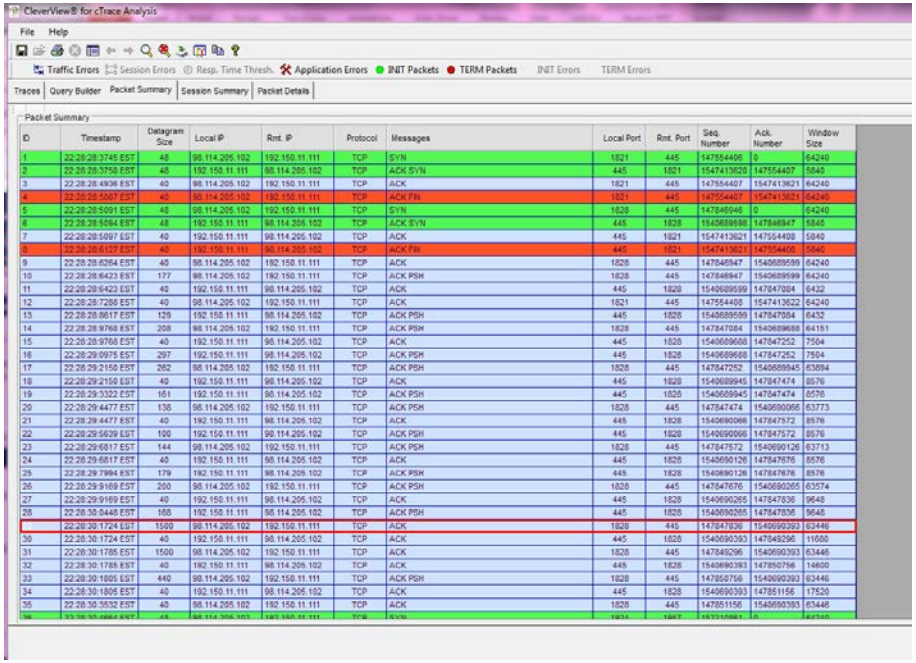
Forensic Tools

- IDS (Intrusion Detection System) attempts to detect activity that violates an organization's security policy
- Firewall allows or disallows traffic to or from specific networks, machine addresses and port numbers
- Network Forensic Analysis Tools (NFAT) synergizes with IDSs and Firewalls.
  - Preserves long term record of network traffic
  - Allows quick analysis of trouble spots identified by IDSs and Firewalls
    - NFATs must do the following:
      - Capture network traffic
      - Analyze network traffic according to user needs
      - Allow system users discover useful and interesting things about the analyzed traffic



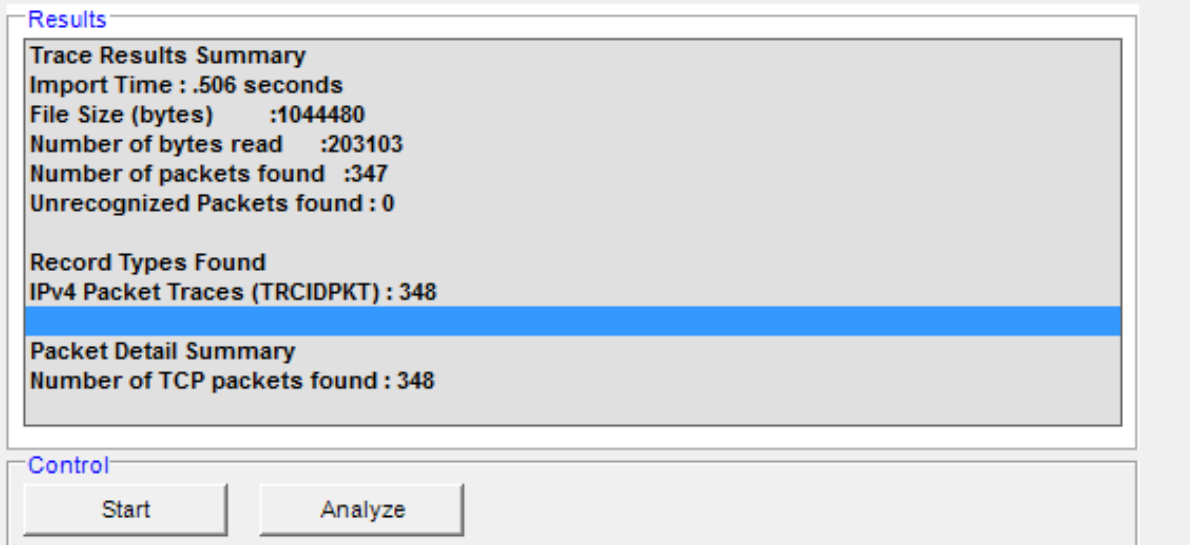
NFAT Tasks

- Traffic Capture
  - What is the policy?
  - What is the traffic of interest?
  - Internal/External?
  - Collect packets
  - Traffic Analysis
  - Organize traffic by session
  - Protocol Parsing and analysis
  - Check for strings, use expert systems for analysis
- Interacting with NFAT
  - Appropriate user interfaces, reports, examine large quantities of information and make it manageable



PCAP Attack Situation*

The network traffic captured relates to an automated malware attack that exploits the Windows Local Security Authority (LSA) Remote Procedure Call (RPC) service of the victim host named “V.I.D.C.A.M.”, IP address 192.150.11.111, compromising the IPC$ share. Once the share is exploited, a script is invoked, causing a connection to an FTP server named “NzmxFtpd” and the acquisition of a file, ssms.exe.



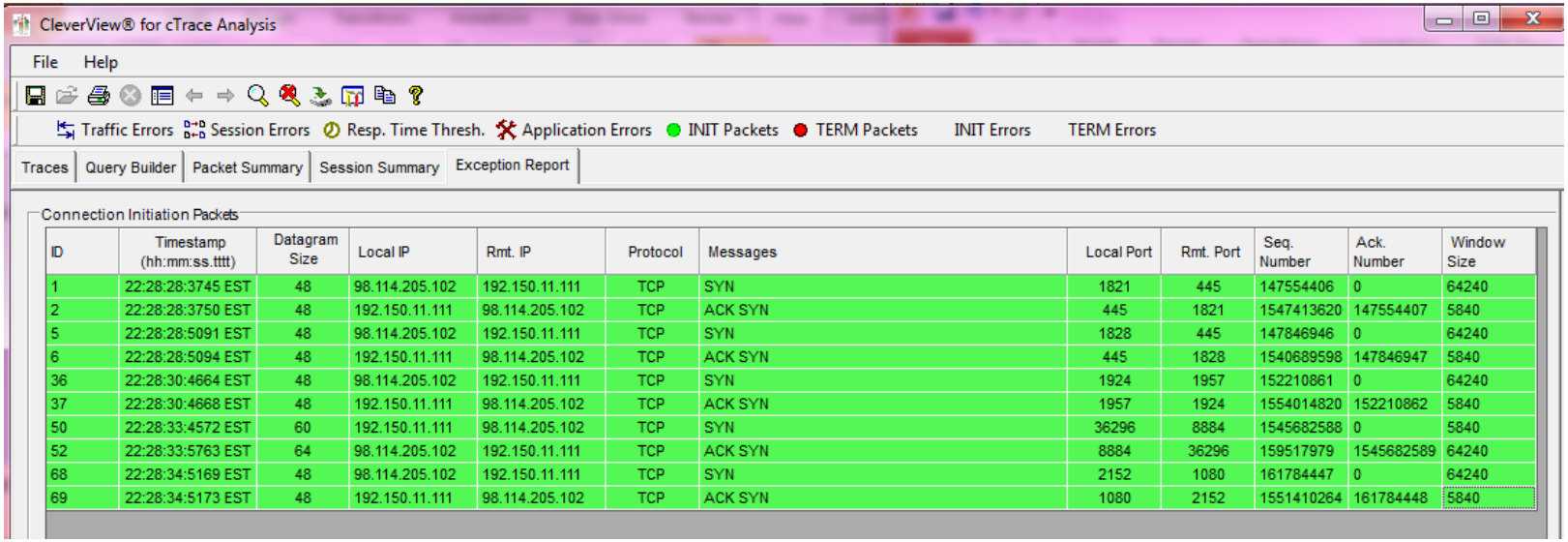
* Excerpts from the HONEYPOT PROJECT 2010 Forensic Challenge

What Can You Learn from the Trace?

- Which systems (i.e. IP addresses) are involved?
- What can you find out about the attacking host (e.g., where is it located)?
- How many TCP sessions are contained in the dump file?
- How long did it take to perform the attack?
- Which operating system was targeted by the attack? And which service? Which vulnerability?
- Can you sketch an overview of the general actions performed by the attacker?
- What specific vulnerability was attacked?
- What actions does the shellcode perform?

What Can You Learn from the Trace?

Which systems (i.e. IP addresses) are involved?



ID	Timestamp (hh:mm:ss.tttt)	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	22:28:28:3745 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1821	445	147554406	0	64240
2	22:28:28:3750 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1821	1547413620	147554407	5840
5	22:28:28:5091 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1828	445	147846946	0	64240
6	22:28:28:5094 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1828	1540689598	147846947	5840
36	22:28:30:4664 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1924	1957	152210861	0	64240
37	22:28:30:4668 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	1957	1924	1554014820	152210862	5840
50	22:28:33:4572 EST	60	192.150.11.111	98.114.205.102	TCP	SYN	36296	8884	1545682588	0	5840
52	22:28:33:5763 EST	64	98.114.205.102	192.150.11.111	TCP	ACK SYN	8884	36296	159517979	1545682589	64240
68	22:28:34:5169 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	2152	1080	161784447	0	64240
69	22:28:34:5173 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	1080	2152	1551410264	161784448	5840

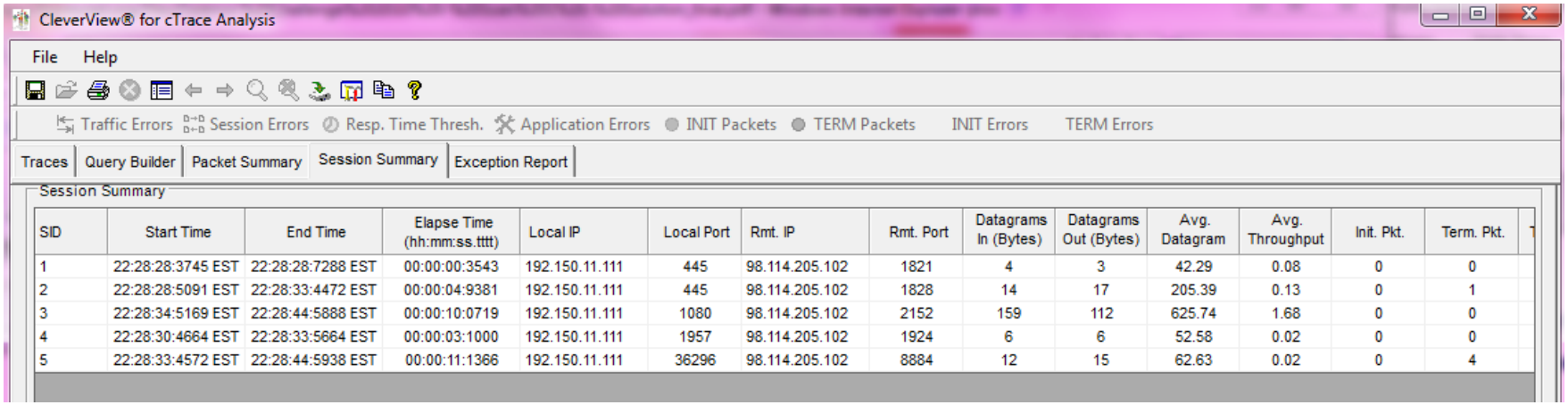
Attacker – 98.114.205.102
Destination – 192.150.11.111

What Can You Learn from the Trace?

What can you find out about the attacking host (e.g., where is it located)?

What Can You Learn from the Trace?

How many TCP sessions are contained in the dump file?



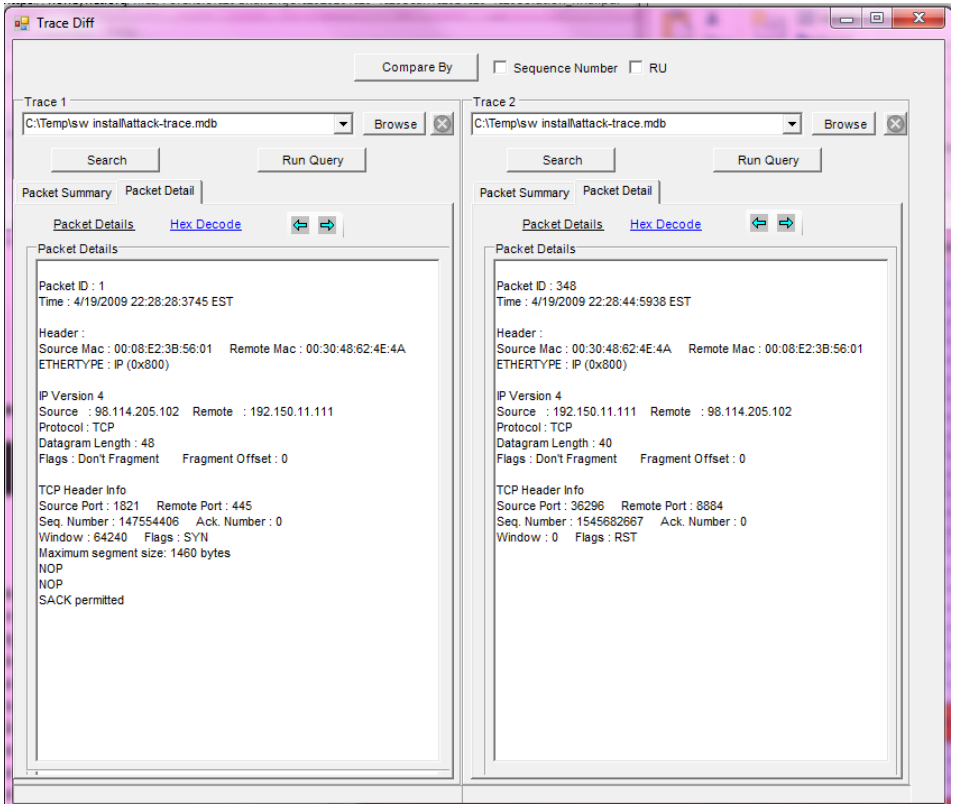
SID	Start Time	End Time	Elapse Time (hh:mm:ss.tttt)	Local IP	Local Port	Rmt. IP	Rmt. Port	Datagrams In (Bytes)	Datagrams Out (Bytes)	Avg. Datagram	Avg. Throughput	Init. Pkt.	Term. Pkt.
1	22:28:28:3745 EST	22:28:28:7288 EST	00:00:00:3543	192.150.11.111	445	98.114.205.102	1821	4	3	42.29	0.08	0	0
2	22:28:28:5091 EST	22:28:33:4472 EST	00:00:04:9381	192.150.11.111	445	98.114.205.102	1828	14	17	205.39	0.13	0	1
3	22:28:34:5169 EST	22:28:44:5888 EST	00:00:10:0719	192.150.11.111	1080	98.114.205.102	2152	159	112	625.74	1.68	0	0
4	22:28:30:4664 EST	22:28:33:5664 EST	00:00:03:1000	192.150.11.111	1957	98.114.205.102	1924	6	6	52.58	0.02	0	0
5	22:28:33:4572 EST	22:28:44:5938 EST	00:00:11:1366	192.150.11.111	36296	98.114.205.102	8884	12	15	62.63	0.02	0	4

5 Sessions

What Can You Learn from the Trace?

How long did it take to perform the attack?

Duration : 16.219218 seconds
Number of Packets: 348

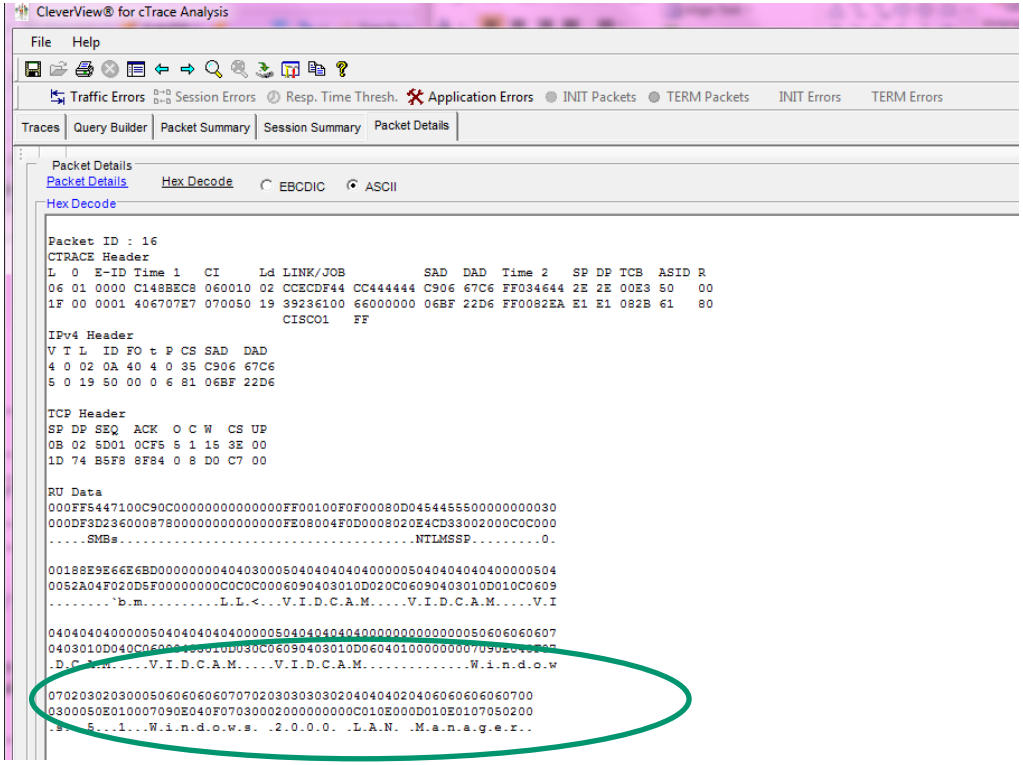


What Can You Learn from the Trace?

Which operating system was targeted by the attack? And which service? Which vulnerability?

OS is Windows XP (windows 5.1)

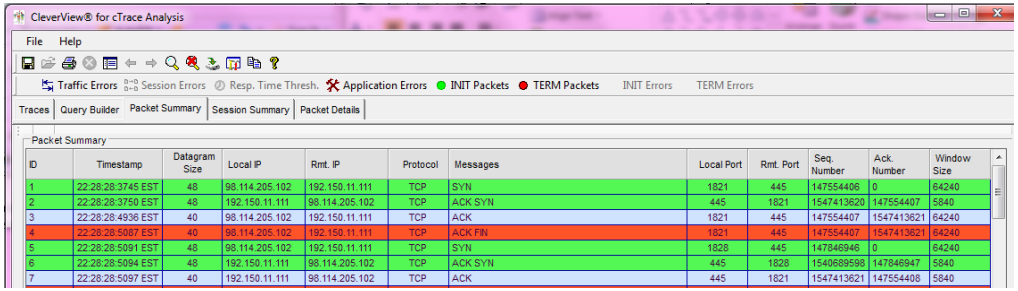
Active Directory Feature



What Can You Learn from the Trace?

Can you sketch an overview of the general actions performed by the attacker?

Recon work is done:



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	22:28:28:3745 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1821	445	147554406	0	64240
2	22:28:28:3750 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1821	1547413620	147554407	5840
3	22:28:28:4936 EST	40	98.114.205.102	192.150.11.111	TCP	ACK	1821	445	147554407	1547413621	64240
4	22:28:28:5087 EST	40	98.114.205.102	192.150.11.111	TCP	ACK FIN	1821	445	147554407	1547413621	64240
5	22:28:28:5091 EST	48	98.114.205.102	192.150.11.111	TCP	SYN	1828	445	147846946	0	64240
6	22:28:28:5094 EST	48	192.150.11.111	98.114.205.102	TCP	ACK SYN	445	1828	1540689598	147846947	5840
7	22:28:28:5097 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1821	1547413621	147554408	5840

Exploit the vulnerable host:

SMB buffer overflow and passes shellcode to bind cmd to a port

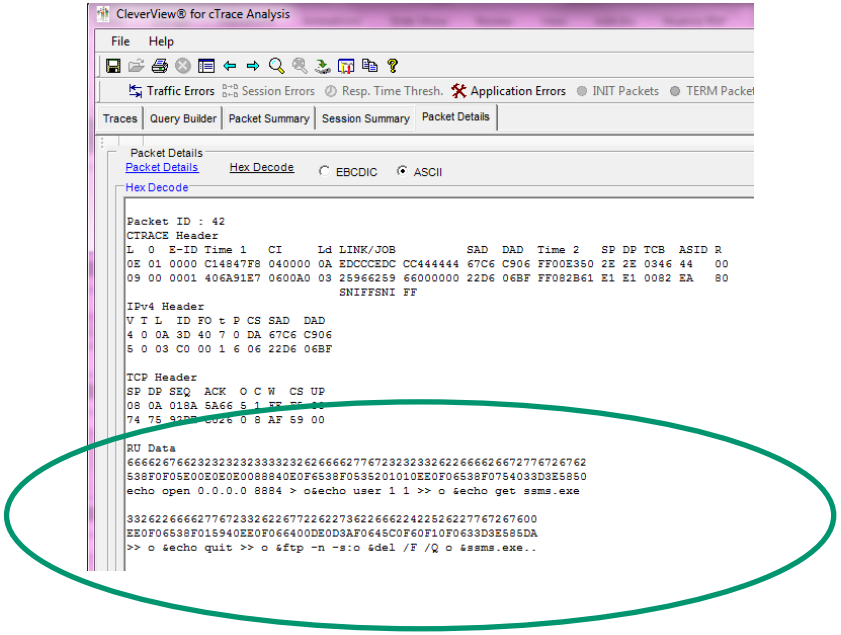
15	22:28:28:9768 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540689688	147847252	7504
16	22:28:29:0975 EST	297	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540689688	147847252	7504
17	22:28:29:2150 EST	262	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847252	1540689945	63894
18	22:28:29:2150 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540689945	147847474	8576
19	22:28:29:3322 EST	161	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540689945	147847474	8576
20	22:28:29:4477 EST	138	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847474	1540690066	63773
21	22:28:29:4477 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690066	147847572	8576
22	22:28:29:5639 EST	100	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690066	147847572	8576
23	22:28:29:6817 EST	144	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847572	1540690126	63713
24	22:28:29:6817 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690126	147847676	8576
25	22:28:29:7994 EST	179	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690126	147847676	8576
26	22:28:29:9169 EST	200	98.114.205.102	192.150.11.111	TCP	ACK PSH	1828	445	147847676	1540690265	63574
27	22:28:29:9169 EST	40	192.150.11.111	98.114.205.102	TCP	ACK	445	1828	1540690265	147847836	9648
28	22:28:30:0448 EST	168	192.150.11.111	98.114.205.102	TCP	ACK PSH	445	1828	1540690265	147847836	9648

What can you learn from the trace?

Can you sketch an overview of the general actions performed by the attacker?

Frame 42:

FTP Download and malware execution instructions are transmitted



What can you learn from the trace?

Can you sketch an overview of the general actions performed by the attacker?

Frame 50:

Victim initiates FTP connection to the attacker and downloads a file name ssms.exe

46	22:28:33:3179 EST	41	192.150.11.111	98.114.205.102	TCP	ACK PSH	1957	1924	1554014822	152210995	5840
54	22:28:33:7239 EST	73	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159517980	1545682589	64240
56	22:28:33:7240 EST	60	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682589	159518001	46
57	22:28:33:8489 EST	74	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159518001	1545682597	64232
58	22:28:33:8489 EST	60	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682597	159518023	46
59	22:28:33:9790 EST	72	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159518023	1545682605	64224
60	22:28:33:9791 EST	58	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682605	159518043	46
61	22:28:34:1115 EST	65	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159518043	1545682611	64218
62	22:28:34:1115 EST	60	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682611	159518056	46
63	22:28:34:2464 EST	71	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159518056	1545682619	64210
64	22:28:34:2465 EST	78	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682619	159518075	46
65	22:28:34:3839 EST	81	98.114.205.102	192.150.11.111	TCP	ACK PSH	8884	36296	159518075	1545682645	64184
66	22:28:34:3840 EST	67	192.150.11.111	98.114.205.102	TCP	ACK PSH	36296	8884	1545682645	159518104	46

Stream

Packet 54….NzmxFtpd owns J0
Packet 59…..User 1 is logged in
Packet 63…..Type is set to I
Packet 65……Port command successful
Packet 67…..Opens Binary data connection
Packet 348….FTP session is closedtransfer complete

What can you learn from the trace?

What specific vulnerability was attacked?

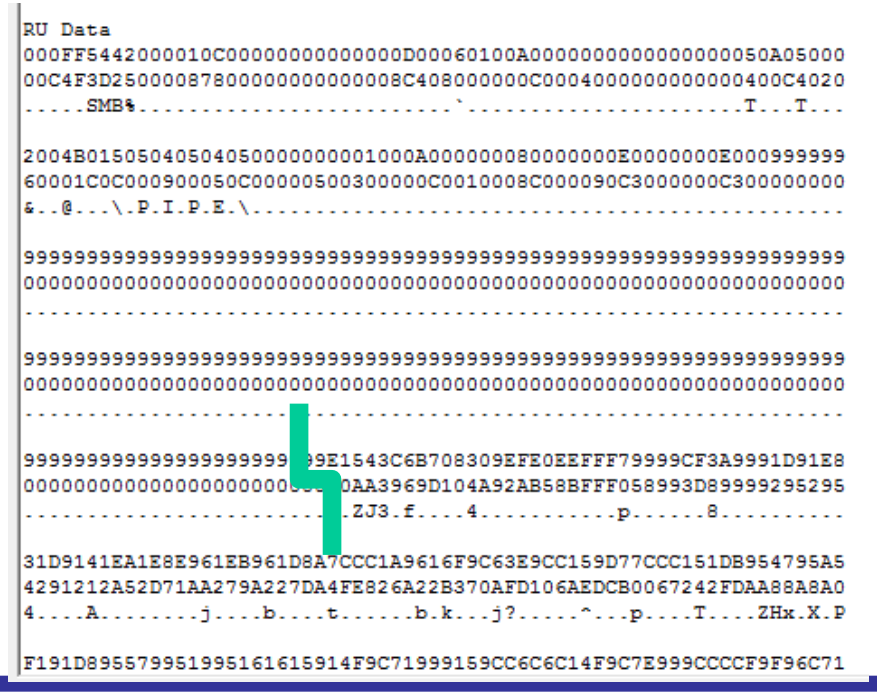
Stack based buffer overflow in certain Active Directory service functions in LSASEV.DLL of the local Security Authority Subsystem Service (LSASS). Exploits a lack of array boundary checking in a LSASS function.

What can you learn from the trace?

What actions does the shellcode perform?

Shellcode was in TCP segments 29, 31, and 33

Tools like Ollydbg and IDA can analyze shellcode further



Common Forensics Mistakes

- Failure to Monitor
  - ICMP Traffic
  - SMTP, POP and IMAP Traffic
  - UseNet Traffic
  - Files saved to external media
  - Web Traffic
  - Senior Executives Traffic
  - Internal IP Traffic
- Failure to PlayBack
  - Encrypted traffic
  - Graphics
  - Modeling and Simulation traffic
- Failure to Detect
  - ICMP Covert Channels
  - UDP Covert Channels
  - HTTP Covert Channels
  - Steganography
  - Erasing Logs
  - File Encryption
  - Binary Trojans
- Failure to Trace:
  - DOS
  - DDOS
  - Spoofed EMail

QUESTIONS?

laurak@aesclever.com
www.aesclever.com
650-617-2400

Our other presentations:

Tuesday, 9:30 am – 10:30 am: Performance Management 101
Tuesday, 3:00 pm - 4:00 pm: Performance Management in a Virtualized Environment
Wednesday 3:00 pm – 4:00 pm: Management Changes in IPv6 – Focus on ICMPv6
Thursday 9:30 am – 10:30 am: Hot Topics in Networking and Security
Thursday 1:30 pm – 2:30 pm: Network Problem Diagnosis with OSA Examples
Thursday 3:00 pm – 4:00 pm: TCP/IP Forensics
Friday 8:00 am – 9:00 pm: Keeping Your Network at Peak Performance as you Virtualize the Data Center
Friday 9:30 am – 10:30 am: Virtualization: New Technologies and Methods to Assure the Health of the Infrastructure