

Introduction to Managed Security Services



DeeDoc Consulting

Presenter: Ola Balogun,
(CISSP, MCSE, CRISC,
CCNP)



Quick managed security services Overview

- Managed Intrusion Detection/Prevention Service
- Managed Firewall
- Security Assessment
- Policy Compliance Audit



What Strategies can I implement to help provide end to end protection and maximum performance for my network ?

C I A

A world map is visible in the background, rendered in a lighter shade of blue than the overall background. The map shows the continents and is centered on the Atlantic Ocean.

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

Threat Management Services (CIA)

- Perimeter Security
- Intrusion detection
- Investigation and forensics
- Privacy/Confidentiality/Integrity
- Auditing/Logging and Alerting
- Operating system hardening
- Application and database security
- Physical Security
- Data Management (Defining critical asset)
- Separation of responsibilities
- Authentication and encryption
- Training

FACTS FROM SANS

www.sans.org/reading_room/whitepapers/threats/system-persistent-baseline-automated-vulnerability-scanning-response-distributed-univ_1886

- Automated Vulnerability Scanning in a distributed Environment test
- The slammer worm doubled in size every 8.5 secs and was able to reach its peak in 3 min conducting 55 million scans per second to seek victims.

Technologies Behind managed security services

- SIEMS - Unified platform to provide clients with a range of services
- ISMS - Set of policies concerned with information security management or IT related risks.

SECURITY INFORMATION EVENTS MANAGEMENT (SIEM)

- Performs four unique functions for the SOC:
 - Security Event Management
 - Log management
 - Customer Reporting
 - Network Forensics

Security Event Management

- Primarily supports the Managed Intrusion Detection Service (MIDS)
- Incoming security alerts are processed, prioritized, persisted (database), and displayed
- Events are highlighted by severity and can be managed and researched by analysts to make security assessments

d_time	customer	facility_name	sever...	signature	direction	s_ip	s_port	t_ip
2004-07-12 19:32:18	Flintkn	midf02s	5	Impossible IP packet	(direction)	12.47.110.206	32626	12.47.110.206
2004-07-12 18:51:05	Lexmark	LMDS1A0L01	4	MS PCT Overflow	(direction)	67.89.212.8	3220	12.155.58.158
2004-07-12 18:45:05	Lexmark	LMDS1A0L01	4	SMTPADDRESS-OVERFLOW	OUT-IN	248.147.86.91	4637	12.155.58.158
2004-07-12 18:41:21	FIRSTCOMMONW...	midfcd1s	5	Outlook malho Quote Attack	(direction)	192.208.45.117	80	12.34.21.153
2004-07-12 18:25:29	NECNY	midn01s	5	Illegal MHTML URL	(direction)	209.66.174.216	80	12.22.103.278
2004-07-12 17:29:52	TowerFederalCre...	midfcd2s	4	AIM / ICQ Messenger Activity	(direction)	12.145.58.158	----	multiple----
2004-07-12 17:29:50	TowerFederalCre...	midfcd1s	4	AIM / ICQ Messenger Activity	(direction)	12.145.58.67	----	multiple----
2004-07-12 17:00:06	Flintkn	midf02s	5	MSSQL 2000 Resolution Overflow	(direction)	32.78.151.4	88	192.168.1.78
2004-07-12 16:51:59	TowerFederalCre...	midfcd2s	4	WinMk Server Response	(direction)	144.144.10.43	----	multiple----
2004-07-12 16:38:48	TowerFederalCre...	midfcd2s	4	eDanky Activity	(direction)	198.74.34.31	80	144.144.10.43
2004-07-12 16:37:26	Lexmark	LMDS1A0L01	4	SMTPADDRESS-OVERFLOW	OUT-IN	69.145.197	3003	192.155.58.158
2004-07-12 16:34:23	CapitalGroup	midfcd2s	5	Missed Packet Count	(direction)	0.0.0.0	----	multiple----
2004-07-12 16:30:01	NECNY	midn01s	5	Missed Packet Count	(direction)	0.0.0.0	0	0.0.0.0
2004-07-12 16:23:47	HesterCounty	midn01s	5	UPnP LOCATION Overflow	(direction)	152.163.208.57	80	12.42.35.2
2004-07-12 16:16:42	Lexmark	LMDS1K1Y008	4	WEBMS-SSL-PCT	OUT-IN	63.238.180.218	8483	192.146.101.152
2004-07-12 16:12:55	John J Haas	midn01s	4	SNMP IOS Configuration Retrieve	(direction)	12.63.159.14	57174	12.144.224.246
2004-07-12 15:38:29	Flintkn	midf01s	5	Illegal MHTML URL	(direction)	202.104.257.173	80	12.47.110.206
2004-07-12 15:38:29	Flintkn	midf07s	5	Illegal MHTML URL	(direction)	202.104.257.173	80	32.78.194.84
2004-07-12 15:12:22	Lexmark	LMDS1K1Y008	5	GENERIC-SHELL-CROWN-TCP	OUT-IN	166.70.99.138	80	192.146.101.24
2004-07-12 15:02:10	Flintkn	midf02s	5	Windows Workstation Service Ove...	(direction)	192.168.0.220	3168	32.78.69.15
2004-07-12 14:25:36	Flintkn	midf02s	4	WWW.bat file	(direction)	32.78.194.84	41098	66.54.38.65
2004-07-12 13:50:10	Lexmark	LMDS1K1Y008	4	WEBMS-SSL-PCT	OUT-IN	217.186.45.212	39043	192.146.101.139
2004-07-12 13:27:04	Lexmark	LMDS1K1Y008	4	WEBMS-SSL-PCT	OUT-IN	81.155.56.176	3170	192.146.101.212
2004-07-12 13:00:28	TowerFederalCre...	midfcd1s	4	WinMk Server Response	(direction)	12.145.58.67	----	multiple----
2004-07-12 12:43:21	TowerFederalCre...	midfcd1s	4	eDanky Activity	(direction)	12.41.160	443	12.145.58.67
2004-07-12 12:40:28	TowerFederalCre...	midfcd1s	4	eDanky Activity	(direction)	216.15.205.76	80	12.145.58.67
2004-07-12 12:37:58	Lexmark	LMDS1K1Y008	4	IBMSITS-HD-ACCESS	OUT-IN	216.240.137.41	80	192.146.101.24
2004-07-12 12:30:07	TowerFederalCre...	midfcd2s	4	Ka2a GET Request	(direction)	69.33.94.22	80	12.145.58.158
2004-07-12 12:12:21	Lexmark	LMDS1K1Y008	4	SMTPADDRESS-OVERFLOW	IN-OUT	192.146.101.70	----	multiple----
2004-07-12 11:33:03	Good Guys	midn01s	5	MSSQL 2000 Resolution Overflow	(direction)	66.295.114.12	1213	66.122.108.34
2004-07-12 11:03:27	GEIndustrial	midn01s	5	FTP realpath Buffer Overflow	(direction)	12.39.64.154	11928	212.52.166.17
2004-07-12 09:23:12	Lexmark	LMDS1K1Y008	4	SMTPADDRESS-OVERFLOW	OUT-IN	12.158.98.113	6616	192.146.101.72
2004-07-12 05:30:02	Lexmark	LMDS1A0L01	4	FTPLONG-RETR	OUT-IN	61.739.107.164	----	multiple----
2004-07-12 04:53:17	Lexmark	LMDS1A0L01	4	FTPLONG-RETR	OUT-IN	61.62.95.172	----	multiple----
2004-07-12 03:38:57	Lexmark	LMDS1K1Y008	4	IBMSITS-HD-ACCESS	OUT-IN	206.176.218.34	80	192.146.101.24
2004-07-12 03:02:18	Lexmark	LMDS1K1Y008	5	GENERIC-SHELL-CROWN-TCP	IN-OUT	172.31.253.244	----	multiple----
2004-07-12 03:00:14	Lexmark	LMDS1K1Y008	5	GENERIC-SHELL-CROWN-TCP	IN-OUT	192.146.101.226	----	multiple----
2004-07-12 02:49:19	Lexmark	LMDS2K1Y008	4	SMTPADDRESS-OVERFLOW	OUT-IN	67.166.110.143	1929	172.31.251.251
2004-07-12 02:46:12	Lexmark	LMDS1K1Y008	4	SMTPADDRESS-OVERFLOW	OUT-IN	67.166.110.143	1929	192.146.101.4
2004-07-11 23:48:19	Lexmark	LMDS1K1Y008	5	GENERIC-SHELL-CROWN-TCP	OUT-IN	128.111.118.43	80	192.146.101.24
2004-07-11 22:39:43	Lexmark	LMDS1K1Y008	4	NOOPSHH-x86-CWTL-TCP	OUT-IN	194.71.11.70	61532	192.146.101.24
2004-07-11 21:54:36	MidFirst	midn01s	5	HS PCT Overflow	(direction)	207.168.119.188	----	multiple----
2004-07-11 21:47:24	MidFirst	midn01s	5	Apache/mod_ssl Worm Buffer Ove...	(direction)	207.168.119.136	40745	12.151.28.212
2004-07-11 20:35:48	Flintkn	midf02s	5	Windows Workstation Service Ove...	(direction)	192.168.1.92	1663	32.78.69.15
2004-07-11 16:19:40	Lexmark	LMDS1K1Y008	4	COMPCD_TMP2	IN-OUT	172.31.73.204	80	66.215.245.184

Customer Reporting

- Daily, weekly, and monthly reports are generated for all customer devices
- Reports are drawn from firewall and IDS events stored in the NSM database
- Elements to develop business intelligence

Network Forensics

- Security analysts utilize a myriad of data sources, including IDS alerts, firewall logs, router logs, host-based messages, and network session logs
- Automated and manual correlation aids investigation, reduces false positives, and provides better reporting to customers

Network Forensics Investigation

- Packet Analysis
- Investigation

The screenshot displays the Wireshark interface with a packet capture filter set to `ip.addr eq and ip.addr eq`. The main packet list shows several SMTP-related packets. Packet 1 is the start of the conversation, and packet 2 is the first data segment. Packet 3 is an acknowledgment (ACK) for the first segment. Packet 4 is the start of the message body. Packet 5 is another acknowledgment (ACK) for the message body. Packet 6 is the retransmission of the message body. Packet 7 is an acknowledgment (ACK) for the retransmission. Packet 8 is the end of the conversation (QUIT).

The packet details pane for packet 2 shows the following structure:

- Frame 1: 11434 bytes on wire (Ethernet II, Src: Oo:12:da:c2:00:00, Dst: 192.168.1.100)
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.100
- Transmission Control Protocol, Src Port: 25000, Dst Port: 25000
- Simple Mail Transfer Protocol

The packet bytes pane shows the raw data of the SMTP message body, which is a plain text email. The email content is as follows:

```
From: [REDACTED]
To: [REDACTED]
Subject: [REDACTED]
Date: [REDACTED]
Message: [REDACTED]
```

The email body text is: `Message accepted for delivery`

DEEDOC MANAGED SERVICES OFFERING

- 24/7 Real-time monitoring service
- Reduce the need to hire, train a security professional
- Helping to prevent costly security and compliance breach with continuous monitoring
- Alerts and assistance with incident response
- Highly qualified security experts & internet engineers
- ICT Control Audits
- Information Security Assessments
- Audits and compliance assessments

Other Aspect of Deedoc Managed Security Offering

- Physical and environmental Security assessments
- Administrative Reviews
- Audits, Risk management and Compliance
- Business Continuity and data availability
- IT Control Audit
- Penetration and vulnerability testing and assessment
- Electronic Data management and E-Recovery services
- Systems and Network Forensics

MAJOR COMPROMISES & ATTACKS IN 2011

- Some examples:
- RSA
- CITI
- PLAYSTATION
- BESTBUY
- CHASE
- UNIVERSAL MUSIC STUDIO
- DATA SECURITY BREACH AT SK COMM. SOUTH KOREA
- ZIMBABWE STOCK EXCHANGE HACKED
- AVENGE ASSANGE BY ANONYMOUS (Operation Payback)

IS INFORMATION SECURITY PURELY A TECHNOLOGICAL ISSUE ?

ICT Security has evolved : Cyber warfare and attacks have been Growing for many reason today:

- Social an cultural (Anonymous – Group)
- Religious
- Espionage
- Economic
- Criminal
- Script kiddies

WHAT IS DEEDOC/CNC OFFERING TO ITS CUSTOMERS

- Open Source project dedicated to helping organizations understand and improve security provisions
- Do you want to maintain control of Business–Critical Systems?
- Do you want to Integrate information security into business process.
- Cost cutting security management overview
- Average analyst security experience of 5 yrs with security certifications such as CISSP,CRISC,CCNP.
- Security from a global perspective and not just technology
- A driven partner, proactive with 24/7 support