IDS Report for Monday 9-26-05

Item	IP Address	Host Name	Source Port	Destination Port	Total Alerts	Date of last alert	Time of last Alert	Category	Internal or external
Known Virus & Worm IDS Alerts									
Microsoft Plug and Play Overflow	10.86.14.235	BRACHY	1821	445	15	9/26/05	7:43:44	Worm\Virus\Trojan	Internal
Microsoft Plug and Play Overflow	10.86.7.2	XTZ007SA002	1608	445	9	9/26/05	6:56:34	Worm\Virus\Trojan	Internal
Microsoft Plug and Play Overflow	10.86.7.26	XTZ007SA026	3998	445	47	9/26/05	12:45:22	Worm\Virus\Trojan	Internal
RBOT.CBQ Worm Activity	10.86.14.235	BRACHY	1821	445	15	9/26/05	7:43:33	Worm\Virus\Trojan	Internal
RBOT.CBQ Worm Activity	10.86.7.2	XTZ007SA002	1608	445	9	9/26/05	6:56:34	Worm\Virus\Trojan	Internal
RBOT.CBQ Worm Activity	10.86.7.26	XTZ007SA026	3998	445	47	9/26/05	12:45:06	Worm\Virus\Trojan	Internal
TCP SYN Host Sweep	10.128.1.208	XTZ001DS008	2061	445	9	9/26/05	15:02:01	Worm\Virus\Trojan	Internal
TCP SYN Host Sweep	10.128.2.118	XTZ001CT030	1529	445	18	9/26/05	15:03:13	Worm\Virus\Trojan	Internal
TCP SYN Host Sweep	10.128.2.143	XTZ001CT032	1160	445	23	9/26/05	13:59:56	Worm\Virus\Trojan	Internal
TCP SYN Host Sweep	10.86.14.235	BRACHY	2279	445	9	9/26/05	7:43:32	Worm\Virus\Trojan	Internal
TCP SYN Host Sweep	10.86.7.26	XTZ007SA026	4335	445	22	9/26/05	12:45:12	Worm\Virus\Trojan	Internal
Windows RPC DCOM Overflow	10.128.2.112	XTZ001CT183	2963	445	2	9/26/05	13:20:26	Worm\Virus\Trojan	Internal
Windows RPC DCOM Overflow	10.128.2.62	XTZ001CT065	3663	445	1	9/26/05	14:27:17	Worm\Virus\Trojan	Internal
Windows SMB/RPC NoOp Sled	10.86.14.235	BRACHY	1821	445	23	9/26/05	7:43:44	Worm\Virus\Trojan	Internal
Windows SMB/RPC NoOp Sled	10.86.7.2	XTZ007SA002	1608	445	13	9/26/05	6:56:33	Worm\Virus\Trojan	Internal
Windows SMB/RPC NoOp Sled	10.86.7.26	XTZ007SA026	3998	445	127	9/26/05	12:45:21	Worm\Virus\Trojan	Internal
Unusual or Interesting Alerts									
Net Sweep-Echo	10.7.205.228	monitor01.production.com	8	0	3,126	9/26/05	15:26:27	network operations	Internal
Net Sweep-Echo	10.128.1.118	XTZ001SA051	8	0	196	9/26/05	15:23:26	network operations	Internal
Net Sweep-Echo	10.128.40.224	XTZ001WS1098	8	0	502	9/26/05	14:35:13	network operations	Internal
Spyware & P2P IDS Alerts									
180solutions Adware	10.160.1.107	XTZ501WS012	2849	80	2	9/26/05	14:09:21	Spyware \ Adware	External
BitTorrent Client Activity	10.128.9.83	*	11509	6882	81	9/26/05	15:25:09	P2P	External
BitTorrent Client Activity	10.128.9.87	XTZC01LT139	10114	6881	35	9/26/05	10:05:38	P2P	External
Bittorrent Tracker Query	10.128.9.83	*	11501	6969	10	9/26/05	15:17:03	P2P	External
Bittorrent Tracker Query	10.128.9.87	XTZC01LT139	10093	6969	5	9/26/05	9:59:38	P2P	External
Ezula Spyware	10.140.14.110	UMO008WS013	1495	80	86	9/26/05	15:27:30	Spyware \ Adware	External
GAIN Adware Activity	10.93.1.132	XTZ700WS046	4760	80	2	9/26/05	12:03:47	Spyware \ Adware	External
MarketScore Activity	10.40.1.32	UMD001WS665	4521	80	47	9/26/05	14:43:56	Spyware \ Adware	External
New.net Activity	10.46.2.237	UMN002WS034	2767	80	1	9/26/05	9:13:39	Spyware \ Adware	External
SaveNow Spyware	10.155.14.136	UVA022WS088	1840	80	119	9/26/05	9:06:00	Spyware \ Adware	External
ShopAtHomeSelect Agent Activity	10.46.4.113	UMN004WS002	1207	80	1	9/26/05	14:21:31	Spyware \ Adware	External
TSA Activity	10.140.14.110	UMO008WS013	4765	80	2	9/26/05	15:03:27	Spyware \ Adware	External

User	NT User comment field	Date and time of last login	MAC Address of Host	Network Card Manufacture	Host OS (based on TTL)
BK_EXEC	Built-in account for administering the backup EXEC	9/16/05 2:27 PM	00-11-11-7F-DD-2C	Intel Corporation	
			00-0B-CD-0B-E1-73	Compaq (HP)	
			00-0B-CD-9B-69-97	Compaq (HP)	
BK_EXEC	Built-in account for administering the backup EXEC	9/16/05 2:27 PM	00-11-11-7F-DD-2C	Intel Corporation	
			00-0B-CD-0B-E1-73	Compaq (HP)	NT-2000-XP (125)
			00-0B-CD-9B-69-97	Compaq (HP)	
			00-0B-CD-52-BD-95	Compaq (HP)	NT-2000-XP (126)
Linda V.	081205 Medical doctor Anywhere TX	9/26/05 3:09 PM	00-0B-CD-4F-65-1B	Compaq (HP)	NT-2000-XP (125)
Trellis H.	101502 Lab. Tech. - Anywhere, NV	9/26/05 2:47 PM	00-0B-CD-4F-5D-EE	Compaq (HP)	NT-2000-XP (125)
BK_EXEC	Built-in account for administering the backup EXEC	9/16/05 2:27 PM	00-11-11-7F-DD-2C	Intel Corporation	NT-2000-XP (124)
			00-0B-CD-9B-69-97	Compaq (HP)	NT-2000-XP (125)
Darrin K.	012705 Rad Svcs. Dir Anywhere KS	9/26/05 3:28 PM	00-0B-CD-B1-80-0F	Compaq (HP)	NT-2000-XP (125)
Samantha F.	Medical Assistant - Anywhere, NV	9/26/05 2:55 PM	00-0B-CD-AF-CE-F8	Compaq (HP)	NT-2000-XP (125)
BK_EXEC	Built-in account for administering the backup EXEC	9/16/05 2:27 PM	00-11-11-7F-DD-2C	Intel Corporation	
			00-0B-CD-0B-E1-73	Compaq (HP)	
			00-0B-CD-9B-69-97	Compaq (HP)	
Name here	Windows USER Comment field here				*NIX (58)
Name here	Windows USER Comment field here		00-09-6B-58-A7-96	IBM Corporation	
Name here	Windows USER Comment field here	9/26/05 3:36 PM	00-08-02-C0-6A-46	ompaq Computer Corporatio	NT-2000-XP (128)
Name here	Windows USER Comment field here	9/26/05 9:10	00-0A-5E-2D-47-80	3COM Corporation	NT-2000-XP (125)
Name here	Windows USER Comment field here				NT-2000-XP (125)
Name here	Windows USER Comment field here	9/22/05 15:20	00-0E-35-A4-02-79	Intel Corp	NT-2000-XP (125)
Name here	Windows USER Comment field here				NT-2000-XP (125)
Name here	Windows USER Comment field here	9/22/05 15:20	00-0E-35-A4-02-79	Intel Corp	
Name here	Windows USER Comment field here	9/26/05 10:38	00-02-55-7F-BA-A8	IBM Corporation	
Name here	Windows USER Comment field here	9/23/05 9:13	00-0B-CD-2E-A3-A3	Compaq (HP)	NT-2000-XP (124)
Name here	Windows USER Comment field here		00-02-A5-62-5C-9A	ompaq Computer Corporatio	NT-2000-XP (123)
Name here	Windows USER Comment field here	9/23/05 8:17	00-0E-7F-A6-1D-E5	Hewlett Packard	NT-2000-XP (122)
Name here	Windows USER Comment field here		00-11-85-7D-DD-66	Hewlett Packard	
Name here	Windows USER Comment field here		00-0A-5E-30-B7-27	3COM Corporation	NT-2000-XP (122)
Name here	Windows USER Comment field here	9/26/05 10:38	00-02-55-7F-BA-A8	IBM Corporation	NT-2000-XP (123)

Site name (as identified by first 3 octets of the IP address)	Site Contact
Texas North	Eric Smith
Sammons	Jason Smith
Sammons	Jason Smith
Texas North	Eric Smith
Sammons	Jason Smith
Sammons	Jason Smith
Main Datacenter	John Smith
Main Datacenter	John Smith
Main Datacenter	John Smith
Texas North	Eric Smith
Sammons	Jason Smith
Main Datacenter	John Smith
Main Datacenter	John Smith
Texas North	Eric Smith
Sammons	Jason Smith
Sammons	Jason Smith
Eugene	Lee Smith
Main Datacenter	John Smith
Main Datacenter	John Smith
Texas	Thomas L.
Main Datacenter - VPN	John Smith
Main Datacenter - VPN	John Smith
Main Datacenter - VPN	John Smith
Main Datacenter - VPN	John Smith
West Associates	Darrell Smith
Minnesota	Gilbert Smith
West Associates	Jack Smith
Minnesota	Jared Smith
South Texas	Jack Smith
North Associates	Jared Smith
West Associates	Darrell smith