Global Information Assurance Certification Paper

*** Northcutt, freestyle analysis and a bit terse so that it can be hard to follow. Great detects and I loved detect 3. 77 *

SANS Intrusion Detection Immersion Curriculum Practical

Mary Walker, CISSP
April 17, 2000

Ten Detects with Analyses

Detect 1

17:41:10.869573 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:41:10.901489 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:41:40.902558 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:41:40.934643 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:42:10.935925 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:42:10.968053 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:42:40.969082 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:42:41.000982 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:43:11.002317 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:43:11.034499 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:43:41.036655 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:43:41.068867 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:44:11.078585 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:44:11.110489 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:44:41.121811 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:44:41.153868 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:45:11.156902 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:45:11.188732 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:45:41.200155 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:45:41.232880 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]
17:46:11.243366 32.199.195.84.1026 > 32.199.194.77.161: GetRequest(11)[|snmp]
17:46:11.275290 32.199.194.77.161 > 32.199.195.84.1026: GetResponse(11)[|snmp]

Trace mechanism: Windump
Platform: Dell GX1 266
OS: Windows 2000
Intrusion Detection Mechanism: BlackICE Defender

In my work environment, BlackICE Defender alarms constantly that it is detecting UDP port scans from various sources. The trace above is an attempt to analyze one of the scans to determine if it is a false positive. The trace shows 11 reported UDP probes over a period of three minutes. In each case the Windows workstation issues an SNMP GetRequest to IP address 32.199.194.77. The IP address then responds on port 161 with a GetResponse, which seems to be what is setting off BlackICE. This address belongs to an HP 5SI printer running SNMP services. No malicious intent was found, but we're looking into the configuration of both BlackICE and the printer.

Detect 2

18:00:16.694348 32.199.195.84.1360 > 32.199.96.86.135: S 3433017889:3433017889(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:00:16.695209 32.199.96.86.135 > 32.199.195.84.1360: S 927154297:927154297(0) ack 3433017890 win 8760 <mss 1460> (DF)

18:00:16.695419 32.199.195.84.1360 > 32.199.96.86.135: . ack 1 win 17520 (DF)
18:00:16.695895 32.199.195.84.1360 > 32.199.96.86.135: P 1:73(72) ack 1 win 17520 (DF)
18:00:16.698411 32.199.96.86.135 > 32.199.195.84.1360: P 1:61(60) ack 73 win 8688 (DF)
18:00:16.698843 32.199.195.84.1360 > 32.199.96.86.135: P 73:229(156) ack 61 win 17460 (DF)
18:00:16.700945 32.199.96.86.135 > 32.199.195.84.1360: P 61:213(152) ack 229 win 8532 (DF)
18:00:16.701402 32.199.195.84.1360 > 32.199.96.86.135: F 229:229(0) ack 213 win 17308 (DF)
18:00:16.702310 32.199.96.86.135 > 32.199.195.84.1360: . ack 230 win 8532 (DF)
18:00:16.702658 32.199.96.86.135 > 32.199.195.84.1360: F 213:213(0) ack 230 win 8532 (DF)
18:00:16.702797 32.199.195.84.1360 > 32.199.96.86.135: . ack 214 win 17308 (DF)
18:00:16.706252 32.199.195.84.1361 > 32.199.96.86.1816: S 3433073399:3433073399(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:00:16.707046 32.199.96.86.1816 > 32.199.195.84.1361: S 927154310:927154310(0) ack 3433073400 win 8760 <mss 1460> (DF)
18:00:16.707210 32.199.195.84.1361 > 32.199.96.86.1816: . ack 1 win 17520 (DF)
18:00:16.707719 32.199.195.84.1361 > 32.199.96.86.1816: P 1:73(72) ack 1 win 17520 (DF)
18:00:16.714706 32.199.96.86.1816 > 32.199.195.84.1361: P 1:61(60) ack 73 win 8688 (DF)
18:00:16.714998 32.199.195.84.1361 > 32.199.96.86.1816: P 73:157(84) ack 61 win 17460 (DF)
18:00:16.719871 32.199.96.86.1816 > 32.199.195.84.1361: P 61:129(68) ack 157 win 8604 (DF)
18:00:16.723074 32.199.195.84.1362 > 32.199.96.86.1816: S 3433130777:3433130777(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:00:16.723793 32.199.96.86.1816 > 32.199.195.84.1362: S 927154327:927154327(0) ack 3433130778 win 8760 <mss 1460> (DF)
18:00:16.723917 32.199.195.84.1362 > 32.199.96.86.1816: . ack 1 win 17520 (DF)
18:00:16.725688 32.199.195.84.1362 > 32.199.96.86.1816: P 1:123(122) ack 1 win 17520 (DF)
18:00:16.731766 32.199.96.86.1816 > 32.199.195.84.1362: P 1:167(166) ack 123 win 8638 (DF)
18:00:16.734187 32.199.195.84.1362 > 32.199.96.86.1816: P 123:291(168) ack 167 win 17354 (DF)
18:00:16.734368 32.199.195.84.1362 > 32.199.96.86.1816: P 291:403(112) ack 167 win 17354 (DF)
18:00:16.735955 32.199.96.86.1816 > 32.199.195.84.1362: . ack 403 win 8358 (DF)
18:00:16.853405 32.199.195.84.1361 > 32.199.96.86.1816: . ack 129 win 17392 (DF)
18:00:16.920328 32.199.96.86.1816 > 32.199.195.84.1362: P 167:263(96) ack 403 win 8358 (DF)
18:00:17.053759 32.199.195.84.1362 > 32.199.96.86.1816: . ack 263 win 17258 (DF)
18:00:21.978930 32.199.195.84.1365 > 32.199.96.86.135: S 3434505040:3434505040(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:00:21.980349 32.199.96.86.135 > 32.199.195.84.1365: S 927154373:927154373(0) ack 3434505041 win 8760 <mss 1460> (DF)
18:00:21.980531 32.199.195.84.1365 > 32.199.96.86.135: . ack 1 win 17520 (DF)
18:00:21.981074 32.199.195.84.1365 > 32.199.96.86.135: P 1:73(72) ack 1 win 17520 (DF)
18:00:21.983080 32.199.96.86.135 > 32.199.195.84.1365: P 1:61(60) ack 73 win 8688 (DF)
18:00:21.983501 32.199.195.84.1365 > 32.199.96.86.135: P 73:229(156) ack 61 win 17460 (DF)
18:00:21.985193 32.199.96.86.135 > 32.199.195.84.1365: P 61:213(152) ack 229 win 8532 (DF)
18:00:21.985589 32.199.195.84.1365 > 32.199.96.86.135: F 229:229(0) ack 213 win 17308 (DF)
18:00:21.986520 32.199.96.86.135 > 32.199.195.84.1365: . ack 230 win 8532 (DF)
18:00:21.986841 32.199.96.86.135 > 32.199.195.84.1365: F 213:213(0) ack 230 win 8532 (DF)
18:00:21.986979 32.199.195.84.1365 > 32.199.96.86.135: . ack 214 win 17308 (DF)
18:00:21.991142 32.199.195.84.1366 > 32.199.96.86.1857: S 3434545680:3434545680(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:00:21.991830 32.199.96.86.1857 > 32.199.195.84.1366: S 927154390:927154390(0) ack 3434545681 win 8760 <mss 1460> (DF)
18:00:21.991988 32.199.195.84.1366 > 32.199.96.86.1857: . ack 1 win 17520 (DF)
18:00:21.993260 32.199.195.84.1366 > 32.199.96.86.1857: P 1:123(122) ack 1 win 17520 (DF)
18:00:21.998874 32.199.96.86.1857 > 32.199.195.84.1366: P 1:167(166) ack 123 win 8638 (DF)
18:00:22.001710 32.199.195.84.1366 > 32.199.96.86.1857: P 123:291(168) ack 167 win 17354 (DF)
18:00:22.001964 32.199.195.84.1366 > 32.199.96.86.1857: P 291:435(144) ack 167 win 17354 (DF)
18:00:22.002826 32.199.96.86.1857 > 32.199.195.84.1366: . ack 435 win 8326 (DF)
18:00:22.196356 32.199.96.86.1857 > 32.199.195.84.1366: P 167:359(192) ack 435 win 8326 (DF)
18:00:22.197276 32.199.195.84.1366 > 32.199.96.86.1857: P 435:579(144) ack 359 win 17162 (DF)

18:00:22.224270 32.199.96.86.1857 > 32.199.195.84.1366: P 359:631(272) ack 579 win 8182 (DF)
18:00:22.274690 32.199.195.84.1366 > 32.199.96.86.1857: P 579:723(144) ack 631 win 16890 (DF)
18:00:22.278118 32.199.96.86.1857 > 32.199.195.84.1366: P 631:775(144) ack 723 win 8038 (DF)
18:00:22.278819 32.199.195.84.1366 > 32.199.96.86.1857: P 723:931(208) ack 775 win 16746 (DF)
18:00:22.280427 32.199.96.86.1857 > 32.199.195.84.1366: P 775:903(128) ack 931 win 7830 (DF)
18:00:22.287057 32.199.195.84.1366 > 32.199.96.86.1857: . 931:2391(1460) ack 903 win 16618 (DF)
18:00:22.287165 32.199.195.84.1366 > 32.199.96.86.1857: . 2391:3851(1460) ack 903 win 16618 (DF)
18:00:22.287243 32.199.195.84.1366 > 32.199.96.86.1857: P 3851:4643(792) ack 903 win 16618 (DF)
18:00:22.290747 32.199.96.86.1857 > 32.199.195.84.1366: . ack 3851 win 8760 (DF)
18:00:22.294315 32.199.96.86.1857 > 32.199.195.84.1366: P 903:1047(144) ack 4643 win 7968 (DF)
18:00:22.332096 32.199.195.84.1366 > 32.199.96.86.1857: . 4643:6103(1460) ack 1047 win 16474 (DF)
18:00:22.332250 32.199.195.84.1366 > 32.199.96.86.1857: P 6103:6627(524) ack 1047 win 16474 (DF)
18:00:22.335005 32.199.96.86.1857 > 32.199.195.84.1366: . ack 6627 win 8760 (DF)
18:00:22.340629 32.199.96.86.1857 > 32.199.195.84.1366: P 1047:1223(176) ack 6627 win 8760 (DF)
18:00:22.355551 32.199.195.84.1366 > 32.199.96.86.1857: P 6627:6755(128) ack 1223 win 16298 (DF)
18:00:22.357594 32.199.96.86.1857 > 32.199.195.84.1366: P 1223:1495(272) ack 6755 win 8632 (DF)
18:00:22.374183 32.199.195.84.1366 > 32.199.96.86.1857: P 6755:6979(224) ack 1495 win 17520 (DF)
18:00:22.378788 32.199.96.86.1857 > 32.199.195.84.1366: P 1495:2327(832) ack 6979 win 8408 (DF)
18:00:22.391705 32.199.195.84.1366 > 32.199.96.86.1857: P 6979:7139(160) ack 2327 win 16688 (DF)
18:00:22.393838 32.199.96.86.1857 > 32.199.195.84.1366: P 2327:2503(176) ack 7139 win 8248 (DF)
18:00:22.410351 32.199.195.84.1366 > 32.199.96.86.1857: P 7139:7843(704) ack 2503 win 16512 (DF)
18:00:22.415641 32.199.96.86.1857 > 32.199.195.84.1366: P 2503:3415(912) ack 7843 win 7544 (DF)
18:00:22.456189 32.199.195.84.1366 > 32.199.96.86.1857: P 7843:7955(112) ack 3415 win 17520 (DF)
18:00:22.457830 32.199.96.86.1857 > 32.199.195.84.1366: P 3415:3527(112) ack 7955 win 7432 (DF)
18:00:22.461218 32.199.195.84.1366 > 32.199.96.86.1857: P 7955:8051(96) ack 3527 win 17408 (DF)
18:00:22.462776 32.199.96.86.1857 > 32.199.195.84.1366: P 3527:3639(112) ack 8051 win 7336 (DF)
18:00:22.477618 32.199.195.84.1366 > 32.199.96.86.1857: P 8051:8259(208) ack 3639 win 17296 (DF)
18:00:22.482333 32.199.96.86.1857 > 32.199.195.84.1366: P 3639:3911(272) ack 8259 win 8760 (DF)
18:00:22.487715 32.199.195.84.1366 > 32.199.96.86.1857: P 8259:8387(128) ack 3911 win 17024 (DF)
18:00:22.489782 32.199.96.86.1857 > 32.199.195.84.1366: P 3911:4039(128) ack 8387 win 8632 (DF)
18:00:22.526155 32.199.195.84.1366 > 32.199.96.86.1857: P 8387:8499(112) ack 4039 win 16896 (DF)
18:00:22.530532 32.199.96.86.1857 > 32.199.195.84.1366: . 4039:5499(1460) ack 8499 win 8520 (DF)
18:00:22.531754 32.199.96.86.1857 > 32.199.195.84.1366: . 5499:6959(1460) ack 8499 win 8520 (DF)
18:00:22.531957 32.199.195.84.1366 > 32.199.96.86.1857: . ack 6959 win 17520 (DF)
18:00:22.532334 32.199.96.86.1857 > 32.199.195.84.1366: P 6959:7655(696) ack 8499 win 8520 (DF)
18:00:22.661871 32.199.195.84.1366 > 32.199.96.86.1857: . ack 7655 win 16824 (DF)
18:00:37.144157 32.199.195.84.1362 > 32.199.96.86.1816: P 403:515(112) ack 263 win 17258 (DF)
18:00:37.224776 32.199.96.86.1816 > 32.199.195.84.1362: . 263:1723(1460) ack 515 win 8246 (DF)
18:00:37.225985 32.199.96.86.1816 > 32.199.195.84.1362: . 1723:3183(1460) ack 515 win 8246 (DF)
18:00:37.226127 32.199.195.84.1362 > 32.199.96.86.1816: . ack 3183 win 17520 (DF)
18:00:37.227210 32.199.96.86.1816 > 32.199.195.84.1362: . 3183:4643(1460) ack 515 win 8246 (DF)
18:00:37.228579 32.199.96.86.1816 > 32.199.195.84.1362: P 4643:6103(1460) ack 515 win 8246 (DF)
18:00:37.228753 32.199.195.84.1362 > 32.199.96.86.1816: . ack 6103 win 17520 (DF)
18:00:37.231947 32.199.96.86.1816 > 32.199.195.84.1362: . 6103:7563(1460) ack 515 win 8246 (DF)
18:00:37.233185 32.199.96.86.1816 > 32.199.195.84.1362: . 7563:9023(1460) ack 515 win 8246 (DF)
18:00:37.233400 32.199.195.84.1362 > 32.199.96.86.1816: . ack 9023 win 17520 (DF)
18:00:37.234409 32.199.96.86.1816 > 32.199.195.84.1362: . 9023:10483(1460) ack 515 win 8246 (DF)
18:00:37.235685 32.199.96.86.1816 > 32.199.195.84.1362: P 10483:11943(1460) ack 515 win 8246 (DF)
18:00:37.235865 32.199.195.84.1362 > 32.199.96.86.1816: . ack 11943 win 17520 (DF)
18:00:37.236937 32.199.96.86.1816 > 32.199.195.84.1362: . 11943:13403(1460) ack 515 win 8246 (DF)
18:00:37.238200 32.199.96.86.1816 > 32.199.195.84.1362: . 13403:14863(1460) ack 515 win 8246 (DF)
18:00:37.238359 32.199.195.84.1362 > 32.199.96.86.1816: . ack 14863 win 17520 (DF)
18:00:37.240674 32.199.96.86.1816 > 32.199.195.84.1362: . 14863:16323(1460) ack 515 win 8246 (DF)
18:00:37.241905 32.199.96.86.1816 > 32.199.195.84.1362: P 16323:17783(1460) ack 515 win 8246 (DF)
18:00:37.242079 32.199.195.84.1362 > 32.199.96.86.1816: . ack 17783 win 17520 (DF)
18:00:37.243135 32.199.96.86.1816 > 32.199.195.84.1362: . 17783:19243(1460) ack 515 win 8246 (DF)

18:00:37.244418 32.199.96.86.1816 > 32.199.195.84.1362: . 19243:20703(1460) ack 515 win 8246 (DF)
18:00:37.244581 32.199.195.84.1362 > 32.199.96.86.1816: . ack 20703 win 17520 (DF)
18:00:37.245699 32.199.96.86.1816 > 32.199.195.84.1362: . 20703:22163(1460) ack 515 win 8246 (DF)
18:00:37.247041 32.199.96.86.1816 > 32.199.195.84.1362: P 22163:23623(1460) ack 515 win 8246 (DF)
18:00:37.247219 32.199.195.84.1362 > 32.199.96.86.1816: . ack 23623 win 17520 (DF)
18:00:37.248269 32.199.96.86.1816 > 32.199.195.84.1362: . 23623:25083(1460) ack 515 win 8246 (DF)
18:00:37.249592 32.199.96.86.1816 > 32.199.195.84.1362: . 25083:26543(1460) ack 515 win 8246 (DF)
18:00:37.249751 32.199.195.84.1362 > 32.199.96.86.1816: . ack 26543 win 17520 (DF)
18:00:37.250822 32.199.96.86.1816 > 32.199.195.84.1362: . 26543:28003(1460) ack 515 win 8246 (DF)
18:00:37.252082 32.199.96.86.1816 > 32.199.195.84.1362: P 28003:29463(1460) ack 515 win 8246 (DF)
18:00:37.252256 32.199.195.84.1362 > 32.199.96.86.1816: . ack 29463 win 17520 (DF)
18:00:37.253345 32.199.96.86.1816 > 32.199.195.84.1362: . 29463:30923(1460) ack 515 win 8246 (DF)
18:00:37.254602 32.199.96.86.1816 > 32.199.195.84.1362: . 30923:32383(1460) ack 515 win 8246 (DF)
18:00:37.254759 32.199.195.84.1362 > 32.199.96.86.1816: . ack 32383 win 17520 (DF)
18:00:37.255849 32.199.96.86.1816 > 32.199.195.84.1362: . 32383:33843(1460) ack 515 win 8246 (DF)
18:00:37.257108 32.199.96.86.1816 > 32.199.195.84.1362: P 33843:35303(1460) ack 515 win 8246 (DF)
18:00:37.257260 32.199.195.84.1362 > 32.199.96.86.1816: . ack 35303 win 17520 (DF)
18:00:37.258373 32.199.96.86.1816 > 32.199.195.84.1362: . 35303:36763(1460) ack 515 win 8246 (DF)
18:00:37.259619 32.199.96.86.1816 > 32.199.195.84.1362: . 36763:38223(1460) ack 515 win 8246 (DF)
18:00:37.259782 32.199.195.84.1362 > 32.199.96.86.1816: . ack 38223 win 17520 (DF)
18:00:37.260857 32.199.96.86.1816 > 32.199.195.84.1362: . 38223:39683(1460) ack 515 win 8246 (DF)
18:00:37.262112 32.199.96.86.1816 > 32.199.195.84.1362: P 39683:41143(1460) ack 515 win 8246 (DF)
18:00:37.262297 32.199.195.84.1362 > 32.199.96.86.1816: . ack 41143 win 17520 (DF)
18:00:37.268010 32.199.96.86.1816 > 32.199.195.84.1362: . 41143:42603(1460) ack 515 win 8246 (DF)
18:00:37.269239 32.199.96.86.1816 > 32.199.195.84.1362: . 42603:44063(1460) ack 515 win 8246 (DF)
18:00:37.269399 32.199.195.84.1362 > 32.199.96.86.1816: . ack 44063 win 17520 (DF)
18:00:37.270470 32.199.96.86.1816 > 32.199.195.84.1362: . 44063:45523(1460) ack 515 win 8246 (DF)
18:00:37.271753 32.199.96.86.1816 > 32.199.195.84.1362: P 45523:46983(1460) ack 515 win 8246 (DF)
18:00:37.271928 32.199.195.84.1362 > 32.199.96.86.1816: . ack 46983 win 17520 (DF)
18:00:37.273015 32.199.96.86.1816 > 32.199.195.84.1362: . 46983:48443(1460) ack 515 win 8246 (DF)
18:00:37.274272 32.199.96.86.1816 > 32.199.195.84.1362: . 48443:49903(1460) ack 515 win 8246 (DF)
18:00:37.274434 32.199.195.84.1362 > 32.199.96.86.1816: . ack 49903 win 17520 (DF)
18:00:37.275535 32.199.96.86.1816 > 32.199.195.84.1362: . 49903:51363(1460) ack 515 win 8246 (DF)
18:00:37.276801 32.199.96.86.1816 > 32.199.195.84.1362: P 51363:52823(1460) ack 515 win 8246 (DF)
18:00:37.276982 32.199.195.84.1362 > 32.199.96.86.1816: . ack 52823 win 17520 (DF)
18:00:37.278009 32.199.96.86.1816 > 32.199.195.84.1362: . 52823:54283(1460) ack 515 win 8246 (DF)
18:00:37.279291 32.199.96.86.1816 > 32.199.195.84.1362: . 54283:55743(1460) ack 515 win 8246 (DF)
18:00:37.279475 32.199.195.84.1362 > 32.199.96.86.1816: . ack 55743 win 17520 (DF)
18:00:37.280516 32.199.96.86.1816 > 32.199.195.84.1362: . 55743:57203(1460) ack 515 win 8246 (DF)
18:00:37.281749 32.199.96.86.1816 > 32.199.195.84.1362: P 57203:58663(1460) ack 515 win 8246 (DF)
18:00:37.281924 32.199.195.84.1362 > 32.199.96.86.1816: . ack 58663 win 17520 (DF)
18:00:37.284281 32.199.96.86.1816 > 32.199.195.84.1362: . 58663:60123(1460) ack 515 win 8246 (DF)
18:00:37.285510 32.199.96.86.1816 > 32.199.195.84.1362: . 60123:61583(1460) ack 515 win 8246 (DF)
18:00:37.285680 32.199.195.84.1362 > 32.199.96.86.1816: . ack 61583 win 17520 (DF)
18:00:37.286738 32.199.96.86.1816 > 32.199.195.84.1362: . 61583:63043(1460) ack 515 win 8246 (DF)
18:00:37.288023 32.199.96.86.1816 > 32.199.195.84.1362: P 63043:64503(1460) ack 515 win 8246 (DF)
18:00:37.288179 32.199.195.84.1362 > 32.199.96.86.1816: . ack 64503 win 17520 (DF)
18:00:37.289292 32.199.96.86.1816 > 32.199.195.84.1362: . 64503:65963(1460) ack 515 win 8246 (DF)
18:00:37.290539 32.199.96.86.1816 > 32.199.195.84.1362: . 65963:67423(1460) ack 515 win 8246 (DF)
18:00:37.290703 32.199.195.84.1362 > 32.199.96.86.1816: . ack 67423 win 17520 (DF)
18:00:37.291792 32.199.96.86.1816 > 32.199.195.84.1362: . 67423:68883(1460) ack 515 win 8246 (DF)
18:00:37.293003 32.199.96.86.1816 > 32.199.195.84.1362: P 68883:70343(1460) ack 515 win 8246 (DF)
18:00:37.293157 32.199.195.84.1362 > 32.199.96.86.1816: . ack 70343 win 17520 (DF)
18:00:37.294260 32.199.96.86.1816 > 32.199.195.84.1362: . 70343:71803(1460) ack 515 win 8246 (DF)
18:00:37.295512 32.199.96.86.1816 > 32.199.195.84.1362: . 71803:73263(1460) ack 515 win 8246 (DF)
18:00:37.295679 32.199.195.84.1362 > 32.199.96.86.1816: . ack 73263 win 17520 (DF)

18:00:37.296769 32.199.96.86.1816 > 32.199.195.84.1362: . 73263:74723(1460) ack 515 win 8246 (DF)
18:00:37.297996 32.199.96.86.1816 > 32.199.195.84.1362: P 74723:76183(1460) ack 515 win 8246 (DF)
18:00:37.298175 32.199.195.84.1362 > 32.199.96.86.1816: . ack 76183 win 17520 (DF)
18:00:37.302899 32.199.96.86.1816 > 32.199.195.84.1362: . 76183:77643(1460) ack 515 win 8246 (DF)
18:00:37.304124 32.199.96.86.1816 > 32.199.195.84.1362: . 77643:79103(1460) ack 515 win 8246 (DF)
18:00:37.304289 32.199.195.84.1362 > 32.199.96.86.1816: . ack 79103 win 17520 (DF)
18:00:37.305354 32.199.96.86.1816 > 32.199.195.84.1362: . 79103:80563(1460) ack 515 win 8246 (DF)
18:00:37.306602 32.199.96.86.1816 > 32.199.195.84.1362: P 80563:82023(1460) ack 515 win 8246 (DF)
18:00:37.306778 32.199.195.84.1362 > 32.199.96.86.1816: . ack 82023 win 17520 (DF)
18:00:37.307867 32.199.96.86.1816 > 32.199.195.84.1362: . 82023:83483(1460) ack 515 win 8246 (DF)
18:00:37.309110 32.199.96.86.1816 > 32.199.195.84.1362: . 83483:84943(1460) ack 515 win 8246 (DF)
18:00:37.309243 32.199.195.84.1362 > 32.199.96.86.1816: . ack 84943 win 17520 (DF)
18:00:37.310453 32.199.96.86.1816 > 32.199.195.84.1362: . 84943:86403(1460) ack 515 win 8246 (DF)
18:00:37.311770 32.199.96.86.1816 > 32.199.195.84.1362: P 86403:87863(1460) ack 515 win 8246 (DF)
18:00:37.311951 32.199.195.84.1362 > 32.199.96.86.1816: . ack 87863 win 17520 (DF)
18:00:37.313094 32.199.96.86.1816 > 32.199.195.84.1362: . 87863:89323(1460) ack 515 win 8246 (DF)
18:00:37.314415 32.199.96.86.1816 > 32.199.195.84.1362: . 89323:90783(1460) ack 515 win 8246 (DF)
18:00:37.314581 32.199.195.84.1362 > 32.199.96.86.1816: . ack 90783 win 17520 (DF)
18:00:37.315646 32.199.96.86.1816 > 32.199.195.84.1362: . 90783:92243(1460) ack 515 win 8246 (DF)
18:00:37.316904 32.199.96.86.1816 > 32.199.195.84.1362: P 92243:93703(1460) ack 515 win 8246 (DF)
18:00:37.317080 32.199.195.84.1362 > 32.199.96.86.1816: . ack 93703 win 17520 (DF)
18:00:37.318151 32.199.96.86.1816 > 32.199.195.84.1362: . 93703:95163(1460) ack 515 win 8246 (DF)
18:00:37.319409 32.199.96.86.1816 > 32.199.195.84.1362: . 95163:96623(1460) ack 515 win 8246 (DF)
18:00:37.319537 32.199.195.84.1362 > 32.199.96.86.1816: . ack 96623 win 17520 (DF)
18:00:37.320668 32.199.96.86.1816 > 32.199.195.84.1362: . 96623:98083(1460) ack 515 win 8246 (DF)
18:00:37.321973 32.199.96.86.1816 > 32.199.195.84.1362: P 98083:99543(1460) ack 515 win 8246 (DF)
18:00:37.322158 32.199.195.84.1362 > 32.199.96.86.1816: . ack 99543 win 17520 (DF)
18:00:37.323189 32.199.96.86.1816 > 32.199.195.84.1362: . 99543:101003(1460) ack 515 win 8246 (DF)
18:00:37.324443 32.199.96.86.1816 > 32.199.195.84.1362: . 101003:102463(1460) ack 515 win 8246 (DF)
18:00:37.324617 32.199.195.84.1362 > 32.199.96.86.1816: . ack 102463 win 17520 (DF)
18:00:37.325682 32.199.96.86.1816 > 32.199.195.84.1362: . 102463:103923(1460) ack 515 win 8246 (DF)
18:00:37.326936 32.199.96.86.1816 > 32.199.195.84.1362: P 103923:105383(1460) ack 515 win 8246
(DF)
18:00:37.327120 32.199.195.84.1362 > 32.199.96.86.1816: . ack 105383 win 17520 (DF)
18:00:37.332486 32.199.96.86.1816 > 32.199.195.84.1362: . 105383:106843(1460) ack 515 win 8246 (DF)
18:00:37.333717 32.199.96.86.1816 > 32.199.195.84.1362: . 106843:108303(1460) ack 515 win 8246 (DF)
18:00:37.333882 32.199.195.84.1362 > 32.199.96.86.1816: . ack 108303 win 17520 (DF)
18:00:37.334946 32.199.96.86.1816 > 32.199.195.84.1362: . 108303:109763(1460) ack 515 win 8246 (DF)
18:00:37.336209 32.199.96.86.1816 > 32.199.195.84.1362: P 109763:111223(1460) ack 515 win 8246
(DF)
18:00:37.336387 32.199.195.84.1362 > 32.199.96.86.1816: . ack 111223 win 17520 (DF)
18:00:37.337467 32.199.96.86.1816 > 32.199.195.84.1362: . 111223:112683(1460) ack 515 win 8246 (DF)
18:00:37.338730 32.199.96.86.1816 > 32.199.195.84.1362: . 112683:114143(1460) ack 515 win 8246 (DF)
18:00:37.338890 32.199.195.84.1362 > 32.199.96.86.1816: . ack 114143 win 17520 (DF)
18:00:37.339989 32.199.96.86.1816 > 32.199.195.84.1362: . 114143:115603(1460) ack 515 win 8246 (DF)
18:00:37.341232 32.199.96.86.1816 > 32.199.195.84.1362: P 115603:117063(1460) ack 515 win 8246
(DF)
18:00:37.341382 32.199.195.84.1362 > 32.199.96.86.1816: . ack 117063 win 17520 (DF)
18:00:37.342492 32.199.96.86.1816 > 32.199.195.84.1362: . 117063:118523(1460) ack 515 win 8246 (DF)
18:00:37.343931 32.199.96.86.1816 > 32.199.195.84.1362: . 118523:119983(1460) ack 515 win 8246 (DF)
18:00:37.344058 32.199.195.84.1362 > 32.199.96.86.1816: . ack 119983 win 17520 (DF)
18:00:37.345008 32.199.96.86.1816 > 32.199.195.84.1362: . 119983:121443(1460) ack 515 win 8246 (DF)
18:00:37.346232 32.199.96.86.1816 > 32.199.195.84.1362: P 121443:122903(1460) ack 515 win 8246
(DF)
18:00:37.346409 32.199.195.84.1362 > 32.199.96.86.1816: . ack 122903 win 17520 (DF)
18:00:37.349676 32.199.96.86.1816 > 32.199.195.84.1362: . 122903:124363(1460) ack 515 win 8246 (DF)

18:00:37.350901 32.199.96.86.1816 > 32.199.195.84.1362: . 124363:125823(1460) ack 515 win 8246 (DF)
18:00:37.351063 32.199.195.84.1362 > 32.199.96.86.1816: . ack 125823 win 17520 (DF)
18:00:37.352131 32.199.96.86.1816 > 32.199.195.84.1362: . 125823:127283(1460) ack 515 win 8246 (DF)
18:00:37.353387 32.199.96.86.1816 > 32.199.195.84.1362: P 127283:128743(1460) ack 515 win 8246 (DF)
18:00:37.353568 32.199.195.84.1362 > 32.199.96.86.1816: . ack 128743 win 17520 (DF)
18:00:37.354654 32.199.96.86.1816 > 32.199.195.84.1362: . 128743:130203(1460) ack 515 win 8246 (DF)
18:00:37.355911 32.199.96.86.1816 > 32.199.195.84.1362: . 130203:131663(1460) ack 515 win 8246 (DF)
18:00:37.356072 32.199.195.84.1362 > 32.199.96.86.1816: . ack 131663 win 17520 (DF)
18:00:37.357153 32.199.96.86.1816 > 32.199.195.84.1362: . 131663:133123(1460) ack 515 win 8246 (DF)
18:00:37.358440 32.199.96.86.1816 > 32.199.195.84.1362: P 133123:134583(1460) ack 515 win 8246 (DF)
18:00:37.358626 32.199.195.84.1362 > 32.199.96.86.1816: . ack 134583 win 17520 (DF)
18:00:37.359668 32.199.96.86.1816 > 32.199.195.84.1362: . 134583:136043(1460) ack 515 win 8246 (DF)
18:00:37.360194 32.199.96.86.1816 > 32.199.195.84.1362: P 136043:136647(604) ack 515 win 8246 (DF)
18:00:37.360324 32.199.195.84.1362 > 32.199.96.86.1816: . ack 136647 win 17520 (DF)
18:00:37.467386 32.199.195.84.1362 > 32.199.96.86.1816: P 515:755(240) ack 136647 win 17520 (DF)
18:00:37.475056 32.199.96.86.1816 > 32.199.195.84.1362: P 136647:137207(560) ack 755 win 8006 (DF)
18:00:37.482831 32.199.195.84.1362 > 32.199.96.86.1816: P 755:899(144) ack 137207 win 16960 (DF)
18:00:37.488170 32.199.96.86.1816 > 32.199.195.84.1362: P 137207:137287(80) ack 899 win 7862 (DF)
18:00:37.494815 32.199.195.84.1362 > 32.199.96.86.1816: P 899:1091(192) ack 137287 win 16880 (DF)
18:00:37.500722 32.199.96.86.1816 > 32.199.195.84.1362: P 137287:137847(560) ack 1091 win 7670 (DF)
18:00:37.508072 32.199.195.84.1366 > 32.199.96.86.1857: P 8499:9139(640) ack 7655 win 16824 (DF)
18:00:37.552229 32.199.96.86.1857 > 32.199.195.84.1366: P 7655:7799(144) ack 9139 win 7880 (DF)
18:00:37.683489 32.199.195.84.1366 > 32.199.96.86.1857: . ack 7799 win 16680 (DF)
18:00:37.683672 32.199.195.84.1362 > 32.199.96.86.1816: . ack 137847 win 16320 (DF)
18:00:37.710169 32.199.195.84.1366 > 32.199.96.86.1857: P 9139:9267(128) ack 7799 win 16680 (DF)
18:00:37.740986 32.199.96.86.1857 > 32.199.195.84.1366: P 7799:7927(128) ack 9267 win 7752 (DF)
18:00:37.741881 32.199.195.84.1366 > 32.199.96.86.1857: P 9267:9347(80) ack 7927 win 16552 (DF)
18:00:37.744263 32.199.96.86.1857 > 32.199.195.84.1366: P 7927:8007(80) ack 9347 win 7672 (DF)
18:00:37.745059 32.199.195.84.1366 > 32.199.96.86.1857: F 9347:9347(0) ack 8007 win 16472 (DF)
18:00:37.746110 32.199.96.86.1857 > 32.199.195.84.1366: . ack 9348 win 7672 (DF)
18:00:37.746294 32.199.96.86.1857 > 32.199.195.84.1366: F 8007:8007(0) ack 9348 win 7672 (DF)
18:00:37.746425 32.199.195.84.1366 > 32.199.96.86.1857: . ack 8008 win 16472 (DF)
18:00:37.752197 32.199.195.84.1362 > 32.199.96.86.1816: P 1091:1171(80) ack 137847 win 16320 (DF)
18:00:37.756691 32.199.96.86.1816 > 32.199.195.84.1362: P 137847:137927(80) ack 1171 win 7590 (DF)
18:00:37.757213 32.199.195.84.1361 > 32.199.96.86.1816: F 157:157(0) ack 129 win 17392 (DF)
18:00:37.757477 32.199.195.84.1362 > 32.199.96.86.1816: F 1171:1171(0) ack 137927 win 16240 (DF)
18:00:37.757878 32.199.96.86.1816 > 32.199.195.84.1361: . ack 158 win 8604 (DF)
18:00:37.758470 32.199.96.86.1816 > 32.199.195.84.1362: . ack 1172 win 7590 (DF)
18:00:37.759266 32.199.96.86.1816 > 32.199.195.84.1361: F 129:129(0) ack 158 win 8604 (DF)
18:00:37.759442 32.199.195.84.1361 > 32.199.96.86.1816: . ack 130 win 17392 (DF)
18:00:37.761373 32.199.96.86.1816 > 32.199.195.84.1362: F 137927:137927(0) ack 1172 win 7590 (DF)
18:00:37.761543 32.199.195.84.1362 > 32.199.96.86.1816: . ack 137928 win 16240 (DF)
18:00:38.485566 32.199.96.86.4284 > 32.199.195.84.1060: udp 8

Trace mechanism: Windump
Platform: Dell GX1 266
OS: Windows 2000
Intrusion Detection Mechanism: BlackICE Defender in cautious mode

Another transaction that BlackICE alarms on in my environment is any outgoing email, identifying the attacking machine as the Exchange server I'm attached to, and identifying the attack as a UDP probe. The trace above is a trace of the outgoing mail transaction down to the packet that causes the BlackICE alarm. There is a series of connections which are set up between my machine at IP 32.199.96.84 and the Exchange

server at 32.199.195.84. Each is set up and terminated normally. For some reason, at the end of the last connection, the Exchange server sends out a UDP packet on port 1060 that is 8 bytes in lenth. This is the packet that BlackICE interprets as a UDP probe. There is no malicious intent or damage done and this is regarded as a false positive. Configuration changes in BlackICE are being examined.

Detect 3

3/27/00 3:29:33AM 0.0.0.0 0 19.104.132.208 80 SYNFlood
SPOOFEDSRC 209.30.121.85
3/27/00 6:18:53AM 168.95.4.90 47295 19.104.132.208 80 HTTP_DotDot URL
/../../download/823/823UM_U/usb.pdf
3/27/00 8:26:44AM 194.2.238.250 0 19.104.132.208 0 IPUnknownProtocol PROTOCOL
54 (NARP)
3/27/00 8:40:28AM 212.244.41.99 0 19.104.132.208 0 PingFlood
3/27/00 8:40:56AM 212.244.41.99 0 19.104.132.208 0 PingFlood
3/27/00 8:41:31AM 212.244.41.99 0 19.104.132.208 0 PingFlood
3/27/00 8:41:32AM 212.244.41.99 0 19.104.132.208 0 PingFlood

Trace mechanism: ISS RealSecure
Platform: Sparc 30
OS: Solaris 2.6
Intrusion Detection Mechanism: ISS RealSecure

Analysis

This report is the one that we have found the most useful of the reports that RealSecure produces and ranks events as high/medium/low priority. We can get more detailed data on each line item from the logs, but this report is very useful for seeing patterns in attacks, which is why I included it in the practical. In this case you are looking at all activity for a particular day. The day started with a SYNflood attempt in the early morning. RealSecure identified the source as spoofed, and suggested an actual source. Then at 6:18, an attempt was made to exploit an HTTP vulnerability. We thought that this was part of a larger scan, since no previous port scans or apparent reconnaissance had been done, but no one else in Motorola saw similar activity. At 8:26, we received a warning on an attempt to connect using port 54, and at 8:40 we started getting a series of Ping floods. These lasted until about 10 AM (but I snipped the duplicate attempts), when we contacted the high school that this was coming from and they told the kid doing it to stop. We still think that the 8:26 attempt was connected to the rest of the attack because of the similarity of the pattern source port and destination port being port 0. We're not sure why the IP address differs, but we think that the kid may have attempted to telnet somewhere else before attempting the attack from school.

Detect 4

20:26:24.544761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:24.544761 209.180.156.136.1077 > 209.181.99.88.21: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:24.604761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:24.604761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 12138674 win 0
20:26:24.604761 209.180.156.136.1077 > 209.181.99.88.21: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:24.604761 209.181.99.88.21 > 209.180.156.136.1077: S 1862177610:1862177610(0) ack 12138674 win 32736 <mss 1460>
20:26:24.704761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:24.704761 209.181.99.88.21 > 209.180.156.136.1077: S 1862177610:1862177610(0) ack 12138674 win 32736 <mss 1460>
20:26:24.704761 209.180.156.136.1077 > 209.181.99.88.21: . ack 1 win 8760 (DF)

20:26:24.784761 209.180.156.136.1077 > 209.181.99.88.21: . ack 1 win 8760 (DF)
20:26:25.114761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:25.284761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:25.284761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:25.404761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:25.814761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:25.924761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:25.924761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:26.034761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:26.514761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:26.604761 209.180.156.136.1076 > 209.181.99.88.20: S 12138673:12138673(0) win 8192 <mss 1460> (DF)
20:26:26.604761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:26.654761 209.181.99.88.20 > 209.180.156.136.1076: R 0:0(0) ack 1 win 0
20:26:27.644761 209.180.156.136.1077 > 209.181.99.88.21: F 1:1(0) ack 1 win 8760 (DF)
20:26:27.684761 209.180.156.136.1077 > 209.181.99.88.21: F 1:1(0) ack 1 win 8760 (DF)
20:26:27.684761 209.181.99.88.21 > 209.180.156.136.1077: . ack 2 win 32735 (DF)
20:26:27.764761 209.181.99.88.21 > 209.180.156.136.1077: . ack 2 win 32735 (DF)
20:26:29.884761 209.181.99.88.21 > 209.180.156.136.1077: F 1:1(0) ack 2 win 32736
20:26:29.924761 209.181.99.88.21 > 209.180.156.136.1077: F 1:1(0) ack 2 win 32736
20:26:29.924761 209.180.156.136.1077 > 209.181.99.88.21: . ack 2 win 8760 (DF)
20:26:29.964761 209.180.156.136.1077 > 209.181.99.88.21: . ack 2 win 8760 (DF)

Trace mechanism: TCPdump
Platform: Intel
OS: Windows 95
Intrusion Detection Mechanism: None

Analysis

This trace is the result of an ISS attempt to FTP to a machine which is not running the service. The machine running the scan, 209.180.156.136 tries to make an FTP connection to 209.181.99.88 several times, but each time receives a reset. Finally, the scanning machine tears the connection down.

Detect 5

22:01:49.611400 209.181.99.35 > 209.180.145.244: icmp: echo request
22:01:49.651386 209.181.99.35 > 209.180.145.244: icmp: echo request
22:01:49.651588 arp who-has 209.180.145.254 tell 209.180.145.244
22:01:49.693781 arp reply 209.180.145.254 is-at 0:0:c:6:62:48
22:01:49.693905 209.180.145.244 > 209.181.99.35: icmp: echo reply
22:01:49.735517 209.180.145.244 > 209.181.99.35: icmp: echo reply
22:01:50.136660 209.181.99.35.1450 > 209.180.145.244.1: S 5868925:5868925(0) win 8192 <mss 1460> (DF)
22:01:50.136881 209.181.99.35.1451 > 209.180.145.244.7: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.137075 209.181.99.35.1452 > 209.180.145.244.9: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.137275 209.181.99.35.1453 > 209.180.145.244.11: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.137474 209.181.99.35.1454 > 209.180.145.244.13: S 5996949:5996949(0) win 8192 <mss 1460> (DF)

22:01:50.137673 209.181.99.35.1455 > 209.180.145.244.15: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.137885 209.181.99.35.1456 > 209.180.145.244.19: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.138091 209.181.99.35.1457 > 209.180.145.244.20: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.138288 209.181.99.35.1458 > 209.180.145.244.21: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.138485 209.181.99.35.1459 > 209.180.145.244.22: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.138686 209.181.99.35.1460 > 209.180.145.244.23: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.138890 209.181.99.35.1461 > 209.180.145.244.25: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.139102 209.181.99.35.1462 > 209.180.145.244.37: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.139310 209.181.99.35.1463 > 209.180.145.244.43: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.139505 209.181.99.35.1464 > 209.180.145.244.53: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.139702 209.181.99.35.1465 > 209.180.145.244.57: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.139899 209.181.99.35.1466 > 209.180.145.244.70: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.140137 209.181.99.35.1467 > 209.180.145.244.77: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.140309 209.181.99.35.1468 > 209.180.145.244.79: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.140517 209.181.99.35.1469 > 209.180.145.244.80: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.140755 209.181.99.35.1470 > 209.180.145.244.87: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.140951 209.181.99.35.1471 > 209.180.145.244.88: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.141146 209.181.99.35.1472 > 209.180.145.244.95: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.141340 209.181.99.35.1473 > 209.180.145.244.101: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.141536 209.181.99.35.1474 > 209.180.145.244.102: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.141732 209.181.99.35.1475 > 209.180.145.244.103: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.141928 209.181.99.35.1476 > 209.180.145.244.104: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.142125 209.181.99.35.1477 > 209.180.145.244.105: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.142365 209.181.99.35.1478 > 209.180.145.244.109: S 5996949:5996949(0) win 8192 <mss 1460> (DF)
22:01:50.142604 209.181.99.35.1479 > 209.180.145.244.110: S 5996917:5996917(0) win 8192 <mss 1460> (DF)
22:01:50.142800 209.181.99.35.1480 > 209.180.145.244.111: S 5996917:5996917(0) win 8192 <mss 1460> (DF)
22:01:50.142995 209.181.99.35.1481 > 209.180.145.244.113: S 5996917:5996917(0) win 8192 <mss 1460> (DF)
22:01:50.274475 209.180.145.244.113 > 209.181.99.35.1481: R 0:0(0) ack 5996918 win 0

Trace mechanism: TCPdump
Platform: Intel
OS: RedHat Linux 5.2
Intrusion Detection Mechanism: none

Analysis

This trace is a TCP port probe which is quite lengthy and is abbreviated here. The attack starts with a ping to ensure that the target is alive, The attempts to connect are very close in time, and sequentially try to access well known TCP ports. The target machine responds with a reset on ports which aren't open, so the probe software determines that where an RST isn't received, the port is open. The RST for port 113 is included as an example. This type of scan is frequently done at our installation to determine where services may be open that aren't required. We also observe this type of scan at our Internet gateways several times a day.

Detect 6

10:13:20.612624 209.181.99.140.1049 > 206.80.192.1.53: 45391+ (34)
10:13:20.672624 206.80.192.1.53 > 209.181.99.140.1049: 45391 1/4/4 (195)
10:13:20.672624 209.181.99.140.1025 > 207.244.124.102.23: S 952416245:952416245(0) win 512 <mss 1460> [tos 0x10]
10:13:20.792624 207.244.124.102.23 > 209.181.99.140.1025: S 3206404002:3206404002(0) ack 952416246 win 8760 <mss 1460> (DF)
10:13:20.792624 209.181.99.140.1025 > 207.244.124.102.23: . ack 1 win 32120 (DF) [tos 0x10]
10:13:20.802624 209.181.99.140.1025 > 207.244.124.102.23: P 1:28(27) ack 1 win 32120 (DF) [tos 0x10]
10:13:20.972624 207.244.124.102.23 > 209.181.99.140.1025: . ack 28 win 8760 (DF)
10:13:21.002624 207.244.124.102.23 > 209.181.99.140.1025: P 1:16(15) ack 28 win 8760 (DF)
10:13:21.012624 209.181.99.140.1025 > 207.244.124.102.23: P 28:40(12) ack 16 win 32120 (DF) [tos 0x10]
10:13:21.132624 207.244.124.102.23 > 209.181.99.140.1025: P 16:31(15) ack 40 win 8760 (DF)
10:13:21.152624 209.181.99.140.1025 > 207.244.124.102.23: . ack 31 win 32120 (DF) [tos 0x10]
10:13:21.272624 207.244.124.102.23 > 209.181.99.140.1025: P 31:52(21) ack 40 win 8760 (DF)
10:13:21.272624 209.181.99.140.1025 > 207.244.124.102.23: P 40:94(54) ack 52 win 32120 (DF) [tos 0x10]
10:13:21.402624 207.244.124.102.23 > 209.181.99.140.1025: P 52:101(49) ack 94 win 8760 (DF)
10:13:21.422624 209.181.99.140.1025 > 207.244.124.102.23: . ack 101 win 32120 (DF) [tos 0x10]
10:13:21.542624 207.244.124.102.23 > 209.181.99.140.1025: P 101:114(13) ack 94 win 8760 (DF)
10:13:21.542624 209.181.99.140.1025 > 207.244.124.102.23: P 94:100(6) ack 114 win 32120 (DF) [tos 0x10]
10:13:21.662624 207.244.124.102.23 > 209.181.99.140.1025: P 114:117(3) ack 100 win 8760 (DF)
10:13:21.682624 209.181.99.140.1025 > 207.244.124.102.23: . ack 117 win 32120 (DF) [tos 0x10]
10:13:22.682624 209.181.99.140.1025 > 207.244.124.102.23: P 100:101(1) ack 117 win 32120 (DF) [tos 0x10]
10:13:22.802624 207.244.124.102.23 > 209.181.99.140.1025: P 117:118(1) ack 101 win 8760 (DF)

Trace mechanism: TCPdump
Platform: Intel
OS: RedHat Linux 5.2
Intrusion Detection Mechanism: None

Analysis

This trace shows the normal setup of a telnet session. First the initiating machine makes a call to DNS (port 53) to locate the target machine, and then the session is iniated with the SYN-SYNACK handshake. This was a normal session, no abnormalities are detected.

Detect 7

Source: http://www.sans.org/y2k/040100.htm
Danicor Technologies Inc, Calgary Alberta, Canada

```
Mar 31 13:07:10 dns3 snort[9658]:
SCAN-SYN FIN: 209.91.87.116:53 -> a.b.c.98:53
--------
[**] SCAN-SYN FIN [**]
03/31-13:07:10.106996 209.91.87.116:53 -> a.b.c.98:53
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x16D8E494 Ack: 0x65E8A466 Win: 0x404
00 00 00 00 00 00 ......

Mar 31 13:07:10 dns1 snort[4415]: spp_portscan:
PORTSCAN DETECTED from 209.91.87.116
Mar 31 13:07:10 dns1 snort[4415]: SCAN-SYN FIN:
209.91.87.116:53 -> a.b.c.34:53
--------
[**] SCAN-SYN FIN [**]
03/31-13:07:10.123109 209.91.87.116:53 -> a.b.c.34:53
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x16D8E494 Ack: 0x65E8A466 Win: 0x404
00 00 00 00 00 00 ......
--------
Mar 31 13:07:16 dns1 snort[4415]: spp_portscan:
portscan status from 209.91.87.116: 1 connections
across 1 hosts: TCP(1), UDP(0) STEALTH
Mar 31 13:07:22 dns1 snort[4415]: spp_portscan:
End of portscan from 209.91.87.116
```

Trace mechanism: Snort
Platform: Unknown
OS: Unknown
Intrusion Detection Mechanism: Snort

Analysis

This trace is a result of the activity which occurred on April 1. Snort detects a portscan in progress and reports that one connection has been made. The source host is identified as 209.91.87.116. This is similar to the behavior that I observed on my home machine, which unfortunately was not running WINdump at the time. Within 5 minutes, I received numerous TCP port probes, SOCKS probes and UDP probes. About the time I was getting ready to contact GIAC, I received the first information on the 911 virus from SANS. I hung back a little in this instance, since I'm new at this, but I won't the next time. It was very obvious that something was going on. My personal firewall, BlackICE defender did an excellent job of alerting me to the situation.

Detect 8

Trace mechanism: RealSecure
Platform: Sparc 30
OS: Solaris 2.6
Intrusion Detection Mechanism: RealSecure

4/9/00 5:16:53PM 99.104.132.100 55908 29.188.106.15 80 HTTP_IE_BAT URL /pub/SPS/MCU/develop/ad05.bat

4/9/00 5:16:53PM	99.104.132.100 55908	29.188.106.15 80	HTTP_IE_BAT URL /pub/SPS/MCU/develop/ad11.bat
4/9/00 5:21:48PM	99.104.132.100 55928	29.188.106.15 80	HTTP_IE_BAT URL /pub/SPS/MCU/ibm/et_asm.bat
4/9/00 7:26:46PM	99.104.132.100 56212	29.188.106.15 80	HTTP_IE_BAT URL /pub/SPS/DSP/software/dr_bub/56100/jpeg/code/decoder/561mk.bat

Analysis

This detect is another entry from our RealSecure event report. This was flagged as a high priority event, but is actually a false positive. The traffic is moving from an internal web development server to a web server on our extranet, and was interpreted as an attack because of the replacement of files. We are trying to adjust RealSecure so that this does not show up as an attack.

Detect 9

4/11/00 11:54:57AM	30.75.135.68 1181	99.104.132.208 80	IPHalfScan
4/11/00 11:55:39AM	30.75.135.68 1181	99.104.132.208 80	TCP_Overlap_Data
4/11/00 11:55:39AM	30.75.135.68 1181	99.104.132.208 80	IPHalfScan

Trace mechanism: RealSecure
Platform: Sparc 30
OS: Solaris 2.6
Intrusion Detection Mechanism: RealSecure

This is an event highlighted as high priority on our RealSecure reporting. The attacker attempts to hit our web server with three attacks in a very brief time span, attempting half-open attacks and fragmented packets. We interpreted this as a denial of service attack, but have not seen any other attacks from this host previously or since. We concluded that this was probably part of a larger attack, but don't have the means to determine if this is the case.

Detect 10

3/26/00 9:55:32PM	19.104.132.208 80	20.168.35.166 33794	Trace_Route
3/26/00 9:56:01PM	19.104.132.208 80	20.168.35.166 33797	Trace_Route
3/26/00 9:56:03PM	19.104.132.208 80	20.168.35.166 33798	Trace_Route
3/26/00 10:09:29PM	19.104.132.208 80	26.66.156.51 61215	Trace_Route
3/26/00 10:22:48PM	19.104.132.208 80	26.66.156.51 61257	Trace_Route
3/26/00 10:23:11PM	19.104.132.208 80	26.66.156.51 61259	Trace_Route
3/26/00 10:23:37PM	19.104.132.208 80	26.66.156.51 61260	Trace_Route
3/27/00 3:10:49AM	19.104.132.208 80	22.114.159.138 36604	Trace_Route
3/27/00 3:58:06AM	19.104.132.208 80	23.228.215.25 42281	Trace_Route
3/27/00 5:08:27AM	19.104.132.208 80	13.76.202.248 44382	Trace_Route

Trace mechanism: RealSecure
Platform: Sparc 30
OS: Solaris 2.6
Intrusion Detection Mechanism: RealSecure

Analysis

This is another example of us attacking ourselves. RealSecure flags this as a medium level problem, but in fact it's traffic from inside our firewall going outbound and the firewall rules just don't match what we told RealSecure. I'm not sure why the source port is showing up as port 80, since traceroute uses DNS and UDP. This is, however, not an attack. I'll be doing some further analysis on what exactly is going on

because of the port question, but I need to get this turned in, so I will leave this as a probable false positive that needs further analysis.

Practical Summary

I installed TCPdump and WINdump on a total of four machines to complete the practical. It was a little difficult to get actual attack data, because we have very few of the RealSeccure engines we've purchased running. I learned that we have no means of coordinating information within the company. I had planned to use the evidence files that BlackICE creates as traces, but could never find a tool that would really read them. That was extremely disappointing and caused me to spend much more time on this than would have been necessary. TCP/WINdump worked just fine, once I realized that I needed to gather my traces there. My biggest regret is that I didn't have WINdump installed on my Win '95 machine on April 1 when the 911 virus scans were hitting. BlackICE certainly alarmed me that something was going on, but the evidence files were worthless. I have really enjoyed working on this exercise, and I'd like to thank all of the people who organized it for helping me learn a great deal in a short time.