VAST 2011 Mini Challenge 2 Answer Guide

Reviewer Guidance

Mini Challenge 2 (MC2) consisted of a scenario about a shipping company and its current project to improve its computer network operations. The following is an excerpt from the scenario description and problem statement:

> *All Freight Corporation is a U.S. company that provides a range of shipping services, focusing on long haul and large-inventory commercial cargo…. Lately, with increased public awareness of cyber attacks, the CEO of All Freight has also asked you, as technical lead of the CNO, to improve the overall situation awareness of the corporate network. …[Y]ou are tasked to develop a situation awareness interface that will give insight as quickly and clearly as possible in order to minimize the burden on the CNO team. The interface should integrate essential information to enable comprehension at a glance.*

The challenge provided three days of data from the corporate network. This information consisted of the following files:

- A file describing the computer network architecture – This documentation includes a list of priority computers. These high priority nodes are essential to All Freight's ability to conduct business.
- Security policy rules
- A firewall log
- An IDS log
- An aggregated file of syslogs for all the hosts on the network
- A Nessus Network Vulnerability Scan Report

An additional file containing PCAP data was also made available to contestants who thought they could use it in their analyses.

Contestants wishing to enter MC2 were asked to provide answers to three questions. Overall, a well-developed solution to MC2 will include: an analysis of the All Freight network and any problems discovered; a description of the analytical approach; an explanation of how the visual analytics facilitates the solution discovery; an explanation of all images from the visual analytics tool(s), and a video that clearly illustrates the analytical approach with the tool in action. The following are the three questions asked, followed by more detailed descriptions of expectations for the answers to each.

> ***MC 2.1 Events of Interest:*** *Using the new situation awareness display(s), what noteworthy events took place for the time period covered in the firewall, IDS and syslog*

*logs? Which events are of concern from a security standpoint? Limit your answer to no more than five noteworthy events. For each event, at least one of the submitted screen shots must be relevant in your explanation of the event. (**Detailed Answer**)*

The noteworthy events from a security standpoint are documented below in the Answer Guide. Events other than the ones listed below would not be part of the ground truth, although there is always a possibility that other events may have been generated by the simulation that could appear important (it's just that we didn't catch them!). If contestants found other events that they deem important from a security standpoint, they need to appropriately justify their answers.

***MC 2.2 Timeliness:** For each event submitted in MC 2.1, how early in the course of the event would your display(s) enable a CNO team member to recognize that the event was noteworthy? For each event, specify the earliest moment of recognition as a timestamp and provide a screen shot at the earliest moment of recognition. Explain how the CNO team member had enough information to determine that the event warranted attention. (**Detailed Answer**)*

The dates and times of the earliest detection can be seen in the Answer Guide. For the explanation, we are really interested in how the visual analytic software facilitated the analysis of the early recognition of the event. Contestants should justify assertions that an event was recognizable.

***MC 2.3 Recommendations:** What are the implications of the events discovered in MC 2.1? What report should the CNO give to the CEO and/or what actions should the CNO take to improve security? (**Short Answer**)*

Obviously, the All Freight networked systems should be patched with the latest system and software updates and security software. A good answer would go beyond general advice to explain specific implications of the events noted in MC 2.1, particularly if the submission does not already provide this information in MC 2.1. A good answer can also include specific recommendations about changing collection to improve insight possible for the All Freight CNO team.

Guidelines for "Detailed" and "Short" answers and videos

A detailed answer is a text description focusing on how the submitting team arrived at the answer, limited to 1000 words (including captions), with a maximum of 5 screen shots. Detailed answers should provide an answer and describe in the process used to arrive at the answer.

A short answer is a text description of the answer and of how the submitting team arrived at the answer. It is limited to 150 words (including captions) and a maximum of 2 screen shots.

All entries are required to include a video with voice narration. Maximum length is 4 minutes for Mini Challenge entries.

Answer Guide

The following pages provide a description of the events that were imbedded in the data provided to participants. Below, we provide excerpts from the datasets and some additional context to assist in evaluating the submissions.

Day 0 Activity

Summary: On Day 0, a Nessus scan was performed on Day 0 and identified security vulnerabilities. No other activity was logged.

Details of the Nessus scan event appear below.

Activity:	Security Scan of AFC Network
Source:	Nessus Security Log
Date/Time:	04/11/2011 1016
Notes:	Below is a single item for each IP address with vulnerabilities. Answers should involve only IP addresses 192.168.2.171 thru 192.168.2.175.
Significance:	This represents a vulnerability to the All Freight Corporation's network security. Five unpatched machines represent a significant risk, which malicious actors take advantage of in subsequent activities.
Data Excerpt:	See below.

192.168.2.171 (through 192.168.2.175)

Security Hole
Arbitrary code can be executed on the remote host through the Microsoft GDI rendering engine.

Description:
The remote host is running a version of Windows that is affected by multiple buffer overflow vulnerabilities when viewing WMF files, which may allow an attacker to execute arbitrary code on the remote host.

To exploit this flaw, an attacker would need to send a malformed WMF file to a user on the remote host and wait for him to open it using an affected Microsoft application.

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms08-071.mspx

Risk factor:
High / CVSS Base Score : 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

Plugin output:
- C:\\WINDOWS\\system32\\Gdi32.dll has not been patched
  Remote version : 5.1.2600.5512
  Should be : 5.1.2600.5698

CVE: CVE-2008-2249,CVE-2008-3465
BID: 32634,32637
Other references: OSVDB:50561,OSVDB:50562,CWE:119,MSFT:MS08-071

Day 1 Activity

Summary: Day 1 includes the following activities:

1. **Denial of service attack from 04/13/2011 1139 (start) – 1251 (end). This is manifested in the firewall log and the IDS log.**
2. **Port scan from 04/13/2011 1115 – 1141. This is manifested in the IDS log.**

Details of these activities are described below.

Activity: 1. Denial of Service Attack
Source: Firewall Log
Date/Time: 04/13/2011 1139 (start) – 1251 (end)
Notes: External systems are attempting to disrupt communications with the web server.
Significance: Substantial. This is an attack on the corporate web server to attempt to disrupt communications.

Start (sample below from host 10.200.150.201)

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
4/13/2011 11:39:51	Info	Built	ASA-session-6-302013	TCP	10.200.150.201	172.20.1.5	4482	80
4/13/2011 11:39:51	Info	Built	ASA-session-6-302013	TCP	10.200.150.201	172.20.1.5	4483	80
4/13/2011 11:39:51	Info	Built	ASA-session-6-302013	TCP	10.200.150.201	172.20.1.5	4484	80
4/13/2011 11:39:51	Info	Built	ASA-session-6-302013	TCP	10.200.150.201	172.20.1.5	4485	80
4/13/2011 11:39:51	Info	Built	ASA-session-6-302013	TCP	10.200.150.201	172.20.1.5	4486	80

End (sample below from host 10.200.150.209)

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
4/13/2011 12:51:10	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.209	172.20.1.5	4319	80
4/13/2011 12:51:10	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.209	172.20.1.5	4320	80
4/13/2011 12:51:10	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.209	172.20.1.5	4313	80
4/13/2011 12:51:10	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.209	172.20.1.5	4321	80
4/13/2011 12:51:10	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.209	172.20.1.5	4318	80

Day 1 Activity (continued)

Activity: 1. Denial of Service Attack
Source: IDS Log
Date/Time: 04/13/2011 1143
Notes: A "restrained" DOS attack begins at 1139 in the firewall log, 1143 in IDS log (small time delay for IDS to process events). It appears that five systems participate at this time.
Significance: Substantial. This is an attack on the corporate web server to attempt to disrupt communications.

```
[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
04/13-11:43:29.787077 10.200.150.207:80 -> 172.20.1.5:56760
TCP TTL:64 TOS:0x0 ID:7722 IpLen:20 DgmLen:88 DF

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
04/13-11:43:36.761013 10.200.150.206:80 -> 172.20.1.5:56762
TCP TTL:64 TOS:0x0 ID:62900 IpLen:20 DgmLen:88 DF

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
04/13-11:43:37.751022 10.200.150.201:80 -> 172.20.1.5:56763
TCP TTL:64 TOS:0x0 ID:5361 IpLen:20 DgmLen:88 DF

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
04/13-11:43:39.752110 10.200.150.209:80 -> 172.20.1.5:56765
TCP TTL:64 TOS:0x0 ID:9251 IpLen:20 DgmLen:88 DF

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
04/13-11:43:44.112440 10.200.150.208:80 -> 172.20.1.5:56766
TCP TTL:64 TOS:0x0 ID:7699 IpLen:20 DgmLen:88 DF
```

Day 1 Activity (continued)

Activity: 2. Port Scan
Source: IDS Log
Date/Time: 04/13/2011 1115 - 1141
Notes: All Freight computers begin port scanning other systems on their own subnet (which is why this is not detected in the Firewall logs).
Significance: Substantial. This suggests a problem within the All Freight network, such as a worm.

Small sample of the log entries follows:

```
[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/13-11:15:10.253703 192.168.2.171:50050 -> 192.168.2.14:33138
TCP TTL:59 TOS:0x0 ID:60899 IpLen:20 DgmLen:60
**U*P**F Seq: 0xC5A810B8  Ack: 0x42B8370A  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/13-11:15:10.253704 192.168.2.171:50050 -> 192.168.2.14:33138
TCP TTL:59 TOS:0x0 ID:60899 IpLen:20 DgmLen:60
**U*P**F Seq: 0xC5A810B8  Ack: 0x42B8370A  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/13-11:15:10.253707 192.168.2.171:50050 -> 192.168.2.15:38169
TCP TTL:49 TOS:0x0 ID:50964 IpLen:20 DgmLen:60
**U*P**F Seq: 0xC5A810B8  Ack: 0x42B8370A  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/13-11:15:10.253708 192.168.2.171:50050 -> 192.168.2.15:38169
TCP TTL:49 TOS:0x0 ID:50964 IpLen:20 DgmLen:60
**U*P**F Seq: 0xC5A810B8  Ack: 0x42B8370A  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/13-11:15:10.253719 192.168.2.171:50050 -> 192.168.2.16:37909
TCP TTL:56 TOS:0x0 ID:19208 IpLen:20 DgmLen:60
**U*P**F Seq: 0xC5A810B8  Ack: 0x42B8370A  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
```

Day 2 Activity

Summary: Day 2 includes the following activities:

1. **Port scan from 04/14/2011 0901 - 0927. This is manifested in the IDS log.**
2. **Port scan from 04/14/2011 1056 - 1228. This is manifested in the IDS log and the firewall log.**
3. **A socially engineered attack that includes multiple parts:**
    a. **SMTP email at 04/14/2011 1123 (first email) and 1323 (response email). This is manifested in the firewall log and optional packet capture (PCAP) data.**
    b. **Remote desktop connection at 04/14/2011 1331. This is documented in the firewall log and is a violation of corporate policy.**
    c. **Authentication to the domain controller for the web server at 04/14/2011 1331. This is documented in the security log.**

Details of these activities are described below.

Activity:	1. Port Scan
Source:	IDS Log
Date/Time:	04/14/2011 0901 - 0927
Notes:	All Freight computers continue port scanning other systems on their own subnet (which is why this is not detected in the Firewall logs). Machines at 192.168.2.174 and .175 are involved.
Significance:	Substantial. This suggests a problem within the All Freight network, such as a worm.

Small sample of the log entries follows:

```
[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-09:01:45.369218 192.168.2.174:52416 -> 192.168.2.14:33185
TCP TTL:50 TOS:0x0 ID:62776 IpLen:20 DgmLen:60
**U*P**F Seq: 0xE89DABB0  Ack: 0x7D1A5A3D  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-09:01:45.369224 192.168.2.174:52416 -> 192.168.2.14:33185
TCP TTL:50 TOS:0x0 ID:62776 IpLen:20 DgmLen:60
**U*P**F Seq: 0xE89DABB0  Ack: 0x7D1A5A3D  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-09:01:45.369403 192.168.2.174:52416 -> 192.168.2.15:38587
TCP TTL:42 TOS:0x0 ID:5718 IpLen:20 DgmLen:60
**U*P**F Seq: 0xE89DABB0  Ack: 0x7D1A5A3D  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
```

```
[Priority: 3]
04/14-09:01:45.369405 192.168.2.174:52416 -> 192.168.2.15:38587
TCP TTL:42 TOS:0x0 ID:5718 IpLen:20 DgmLen:60
**U*P**F Seq: 0xE89DABB0  Ack: 0x7D1A5A3D  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-09:01:45.370139 192.168.2.174:52416 -> 192.168.2.16:33392
TCP TTL:40 TOS:0x0 ID:44439 IpLen:20 DgmLen:60
**U*P**F Seq: 0xE89DABB0  Ack: 0x7D1A5A3D  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
```

Activity: 2. Port Scan
Source: Firewall Log
Date/Time: 04/14/2011 1043
Notes: This port scan attack is from the unpatched workstations which are port scanning internal machines across subnets. The firewall log will only show the internal machines port scanning the servers because they are on another interface on the firewall. Port scans from the same interface will not show up in the logs. An example of the same interface would be a workstation scanning another workstation on the same subnet.
Significance: Substantial. This is the infected workstations attempting to scan for other vulnerable machines.

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.70	55892	1112
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.71	55892	1032
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.72	55892	3689
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.73	55892	9040
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.20	55892	1028
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.21	55892	1028
2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.22	55892	5560

2011-04-14 10:43:35	Info	Build	%ASA-session-6-302013	TCP	192.168.2.175	192.168.1.23	55892	8193
2011-04-14 10:43:36	Info	Teardown	%ASA-session-6-302014	TCP	192.168.2.175	192.168.1.68	55892	443
2011-04-14 10:43:36	Info	Teardown	%ASA-session-6-302014	TCP	192.168.2.175	192.168.1.70	55892	23
2011-04-14 10:43:36	Info	Teardown	%ASA-session-6-302014	TCP	192.168.2.175	192.168.1.71	55892	23

Activity: 2. Port Scan
Source: IDS Log
Date/Time: 04/14/2011 1056 - 1228
Notes: More information supporting the detection of the port scanning.

Small sample of the log entries follows:

```
[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873090 192.168.2.174:44737 -> 192.168.1.74:43895
TCP TTL:47 TOS:0x0 ID:39350 IpLen:20 DgmLen:60
**U*P**F Seq: 0xEB5326B4  Ack: 0x4AF27283  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873182 192.168.2.174:44737 -> 192.168.1.74:43895
TCP TTL:47 TOS:0x0 ID:39350 IpLen:20 DgmLen:60
**U*P**F Seq: 0xEB5326B4  Ack: 0x4AF27283  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873190 192.168.2.174:44737 -> 192.168.1.75:35028
TCP TTL:56 TOS:0x0 ID:48097 IpLen:20 DgmLen:60
**U*P**F Seq: 0xEB5326B4  Ack: 0x4AF27283  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873192 192.168.2.174:44737 -> 192.168.1.75:35028
TCP TTL:56 TOS:0x0 ID:48097 IpLen:20 DgmLen:60
**U*P**F Seq: 0xEB5326B4  Ack: 0x4AF27283  Win: 0xFFFF  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
```

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873193 192.168.2.174:44737 -> 192.168.1.76:43541
TCP TTL:55 TOS:0x0 ID:58422 IpLen:20 DgmLen:60
U*PF Seq: 0xEB5326B4 Ack: 0x4AF27283 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**]
[Priority: 3]
04/14-10:56:12.873194 192.168.2.174:44737 -> 192.168.1.76:43541
TCP TTL:55 TOS:0x0 ID:58422 IpLen:20 DgmLen:60
U*PF Seq: 0xEB5326B4 Ack: 0x4AF27283 Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0

Activity: 3. Socially engineered attack - SMTP Email
Source: Firewall Log
Date/Time: 04/14/2011 1123 (first email), 1323 (response email)
Notes: An email exchange between two AFC employees
Significance: Represents the initiation of a socially engineered attack. Additional information about the activity can be found in the PCAP file during this time.

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
4/14/2011 11:22	Info	Built	ASA-session-6-302013	TCP	192.168.1.6	10.200.150.6	51619	25
4/14/2011 11:22	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.6	192.168.1.6	25	51619
4/14/2011 13:27	Info	Built	ASA-session-6-302013	TCP	10.200.150.6	192.168.1.6	27919	25
4/14/2011 13:28	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.6	192.168.1.6	27919	25
4/14/2011 13:31	Info	Teardown	ASA-session-6-302014	TCP	10.200.150.6	192.168.1.6	25	14681

Activity: 3. Socially engineered attack - Remote Desktop Connection
Source: Firewall Log
Date/Time: 04/14/2011 1331
Notes: Remote Desktop Connection set to alert by emergency if detected from the outside. Remote Desktop connections from outside the network are prohibited by policy, but the network administrator has not blocked the connections on the firewall.
Significance: An emergency alert is raised, however the activity is permitted.

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
4/14/2011 13:31	Emerg	permitted	ASA-session-0-106100	TCP	10.200.150.201	172.20.1.5	4127	3389

Activity: 3. Socially engineered attack - Authentication to Domain Controller
Source: Security Log
Date/Time: 04/14/201 1331 (21:31 Zulu time)
Notes: This is an authentication log for event ID 4634 to the web server corresponding to the unblocked external login.

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E3B0328C30D}'/><EventID>4624</EventID><Version>0</Version><Level>0</Level><Task>12544</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2011-04 14T22:40:02.625000000Z'/><EventRecordID>1434064</EventRecordID><Correlation/><Execution ProcessID='464' ThreadID='1460'/><Channel>Security</Channel><Computer>DC01.AFC.com</Computer><Security/></System><EventData><Data Name='SubjectUserSid'>S-1-0-0</Data><Data Name='SubjectUserName'>-</Data><Data Name='SubjectDomainName'>-</Data><Data Name='SubjectLogonId'>0x0</Data><Data Name='TargetUserSid'>S-1-5-21-2795111079-3225111112-3329435632-1359</Data><Data Name='TargetUserName'>EWS$</Data><Data Name='TargetDomainName'>AFC</Data><Data Name='TargetLogonId'>0x145c37</Data><Data Name='LogonType'>3</Data><Data Name='LogonProcessName'>Kerberos</Data><Data Name='AuthenticationPackageName'>Kerberos</Data><Data Name='WorkstationName'></Data><Data Name='LogonGuid'>{11E02008-AFAD-8908-E6F5-01312553EBAD}</Data><Data Name='TransmittedServices'>-</Data><Data Name='LmPackageName'>-</Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x0</Data><Data Name='ProcessName'>-</Data><Data Name='IpAddress'>172.20.1.5</Data><Data Name='IpPort'>63949</Data></EventData></Event><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E3B0328C30D}'/><EventID>4634</EventID><Version>0</Version><Level>0</Level><Task>12545</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2011-04-14T22:39:59.437500000Z'/><EventRecordID>1434063</EventRecordID><Correlation/><Execution ProcessID='464' ThreadID='1460'/><Channel>Security</Channel><Computer>DC01.AFC.com</Computer><Security/></System><EventData><Data Name='TargetUserSid'>S-1-5-18</Data><Data Name='TargetUserName'>DC01$</Data><Data Name='TargetDomainName'>AFC</Data><Data Name='TargetLogonId'>0x145a35</Data><Data Name='LogonType'>3</Data></EventData></Event>

Day 3 Activity

Summary: Day 3 includes only one activity – the addition of an undocumented computer onto the company internal network. This activity is manifested in the firewall log.

Details of this activity is described below.

Activity: Computer powered on
Source: Firewall Log
Date/Time: 04/14/2011 1323
Notes: First appearance of activity from computer at 192.168.2.251.
Significance: The policy descriptions for AFC state workstations will be assigned IP addresses in the range 192.168.2.25-250. It is unknown what the back story for this machine is, but the appearance of any activity is highly suspicious.

Date/Time	Priority	Operation	Message Code	Protocol	Source IP	Dest IP	Source Port	Dest Port
4/15/2011 14:06	Info	Built	ASA-session-6-302013	TCP	192.168.2.251	172.20.1.5	1033	80