# VAST Challenge 2011 - Mini-Challenge 2

# Computer Network Operations at All Freight Corporation

## Note to Challenge Participants

This document describes important information about the All Freight corporate network operations used in Mini-Challenge 2. It describes the structure and usage of the network and the log data available for the network.

The data files previously provided for this mini-challenge contained examples of the firewall log, intrusion detection system log, security log, and Nessus scan log to illustrate file formats; these files did not contain the actual challenge data. The files provided with this document are the official data for use in the challenge.

In the task description provided with the sample data, it was stated that an XML file would be provided that describes all of the nodes in the network. However, this information is now being provided through the network diagram VAST11MC2\_AFC\_Network.pdf and Table 1.

The following are the additional files provided for this mini-challenge:

1. A file called VAST11MC2\_AFC\_Network.pdf that illustrates the network architecture
2. Log files, which are described in detail later in this document:
   1. Firewall logs. A new log file is created each day. **NOTE: The format of the firewall log has changed from the previously provided example. Please refer to the firewall log file description later in this document.**
   2. Intrusion Detection System logs. A new log file is created each day.
   3. Security logs. A new log file is created each day.
   4. Nessus scan log. One log file is provided.
   5. Packet capture logs, which are provided as optional additional files but are not required for this challenge.

In creating the data formats, the Challenge Committee has taken great care to produce formats that are easily parsed by a wide audience. The intent of the challenge is to focus on the analytics, not on data ingest. If any participants encounter excessive difficulty in ingesting the data, please send feedback to the committee.

For challenge participants with computer security experience, there will be notable absences in the data. The main absence is the lack of information about IP addresses external to the All Freight network. Participants will not be able to extend their investigations with domain name registration lookups (e.g., WHOIS or RIPE) or DNS information. All of the IP addresses and network information used in Mini-Challenge 2 are fictitious.

## Network Description

The file VAST11MC2\_AFC\_Network.pdf contains an illustration of the All Freight Corporation network architecture. The following notations are used in this document and associated network architecture diagram:

* Where an IP is described as 192.168.1.x/24, the “x/24” indicates that “x” can represent any number from 1-255.
* When an IP address is described as 192.168.2.10-250, this indicates that the IP will be one of a range from 192.168.2.10 through 192.168.2.250.

Certain nodes on the network are considered to be high priority nodes because they are critical to the overall operation of All Freight’s business. Other nodes are considered to be of average priority, because loss or damage to those nodes is less likely to be catastrophically disruptive to the company’s business. All Freight Corporation uses virtual machines throughout its network.

The nodes on the All Freight Corporation network are described in Table 1. Nodes outside the ranges 172.x.x.x and 192.x.x.x should be considered external to the All Freight Corporation network.

Table . Nodes on the All Freight Corporation Network

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Address** | **Node Name** | **Node Type** | **Description** | **Priority (High or Normal)** |
| 10.200.150.1 |  | Firewall | Firewall interface to the Internet | High |
| 172.20.1.1 |  | Firewall | Firewall interface to External Web Server | High |
| 172.20.1.5 |  | External Web Server | Web server which hosts All Freight’s external web site | High |
| 192.168.1.16 | Snort IDS | Snort Intrusion Detection System | Snort IDS interface to the network | High |
| 192.168.1.1 |  | Firewall | Firewall interface to data center VLAN | High |
| 192.168.2.1 |  | Firewall | Firewall interface to office VLAN | High |
| 192.168.1.2 | DC01 | DC / DNS / DHCP server | Server running critical network operations: domain controller, domain name server, and dynamic host configuration protocol server | High |
| 192.168.1.3 | HRDB01 | HR Database Server | Server running the database for employee payroll and benefits | High |
| 192.168.1.4 | SRDB01 | Shipping / Routing Database Server | Server containing customer data, including shipping requests and routing information | High |
| 192.168.1.5 | WEB01 | Internal web server | Server that hosts All Freight’s corporate intranet, including company news site and policy and procedure manuals | High |
| 192.168.1.6 | EX01 | Mail server | Server that stores and routes all email that flows into, out of, or internal to All Freight | High |
| 192.168.1.7 | FS01 | File Server | Server that holds shared files used by workers throughout All Freight | High |
| 192.168.1.14 | DC2 | DC / DNS server | Server running critical network operations: domain controller and domain name server | High |
| 192.168.1.50 |  | Firewall log | Server that captures system firewall logs | High |
| 192.168.2.10 through 192.168.2.250 |  | Office workstations | Individual workstation computers located in offices or cubicles throughout All Freight | Normal |

## Common Ports and Their Usage

The following are common ports used on the All Freight network. For a complete list of ports, please refer to <http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers>

* Port 25 – email traffic
* Port 53 – domain name service
* Port 80 – web traffic

## Example Data Flows

The following are example data flows through the All Freight network.

1. **Person outside the All Freight network visits the All Freight Web Server.**
   1. Traffic enters the All Freight network on 10.200.150.1, port 80.
   2. The firewall routes this traffic to the external web server on 172.20.1.5, port 80.
   3. A customer can enter an order or review their account at the <http://www.afc.com> website by selecting new order or order tracking from the page. The traffic originates from the internet and flows to the external web server (172.20.1.5, port 80). The external web server then communicates with the shipping/routing database server (192.168.1.4) to create or retrieve records. This is noted in the firewall log. The shipping/routing database server responds to the external web server, and this activity is recorded in the firewall log. Finally, the external web server returns information back to the originating external source, and this activity is also recorded in the firewall log.
2. **All Freight staff members browse the internet.**
   1. Traffic originates from 192.168.2.10-250.
   2. Traffic flows through the network and exits the firewall on address 10.200.150.1, port 80.
3. **Email from outside the company is sent to an All Freight staff member.**
   1. Email enters the network on 10.200.150.1, port 25.
   2. The firewall routes the traffic to the mail server on 192.168.1.6.
   3. The workstation’s email client communicates with the mail server at 192.168.1.6 to retrieve mail.
4. **Email is sent between All Freight staff members.**
   1. The workstation’s email client communicates with the mail server at 192.168.1.6 to send and receive mail.
5. **Email from inside the All Freight network is sent outside the company.**
   1. The workstation’s email client communicates with the mail server at 192.168.1.6 to send mail.
   2. Based on the destination address of the recipient, the mail server communicates with the recipient’s mail server. All mail going outside the All Freight network is sent from 192.168.1.6, port 25.

## Acceptable Use Policy

The following is the acceptable use policy established for the All Freight network. All company staff members have received training regarding acceptable use of the network.

* The All Freight computer network is to be used for business use only. Personal use of company computing resources is prohibited. Staff members may not use their company computers to access personal email, visit social networking or auction sites, or conduct personal banking activity.
* Employees cannot connect to the All Freight intranet from home or other remote locations. All remote access to the All Freight intranet is blocked, including FTP, telnet, remote login, and remote desktop connections. Thumb drives and other external memory devices not purchased and owned by All Freight cannot be used on company computers. Company-owned thumb drives and external memory that have been removed from company premises must be scanned by a system administrator upon return to the All Freight premises. No personally owned computers or devices may be used on the All Freight network.
* Only company-purchased and approved software may be installed on All Freight computers. Software must be installed by a system administrator. File-sharing software and peer-to-peer communications software are never permitted on All Freight computers.

## Logs

The following logs are available from the All Freight network.

1. Firewall log

The firewall for the All Freight Corporation is a Cisco Adaptive Security Appliance 5510. There are one or more firewall log files for each day. If the firewall log for a day exceeds 512 megabytes, it has been divided into multiple files. These files contain both internal network events and external network events. All internal network events involving traffic between VLANs are logged, and all traffic relating to external networks is logged. This data is captured in a comma-separated values (.csv) file, with the most recent entry at the top. An excerpt from the example file is shown in Figure 1. The types of data captured contained in each firewall record are:

* Date/Time – date and time when activity was performed.
* Syslog priority – the priority of the log message.
* Operation – type of activity being performed.
* Message code – code associated with the message.
* Protocol – connection protocol type.
* Source IP - source IP associated with the activity. This field may be left empty for some log messages.
* Destination IP – the destination IP associated with the activity. This field may be left empty for some log messages.
* Source Hostname - name of the host machine associated with the activity. This field is empty.
* Destination Hostname - name of the host machine associated with the activity. This field is empty.
* Source port - port associated with the source IP in this activity. This field may be left empty for some log messages.
* Destination port - port associated with the destination IP for this activity. This field may be left empty for some log messages.
* Destination service – name of the service associated with the destination port.
* Direction – this field is empty in this dataset.
* Connections built – number of connections built in this operation.
* Connections torn down – number of connections torn down in this operation.

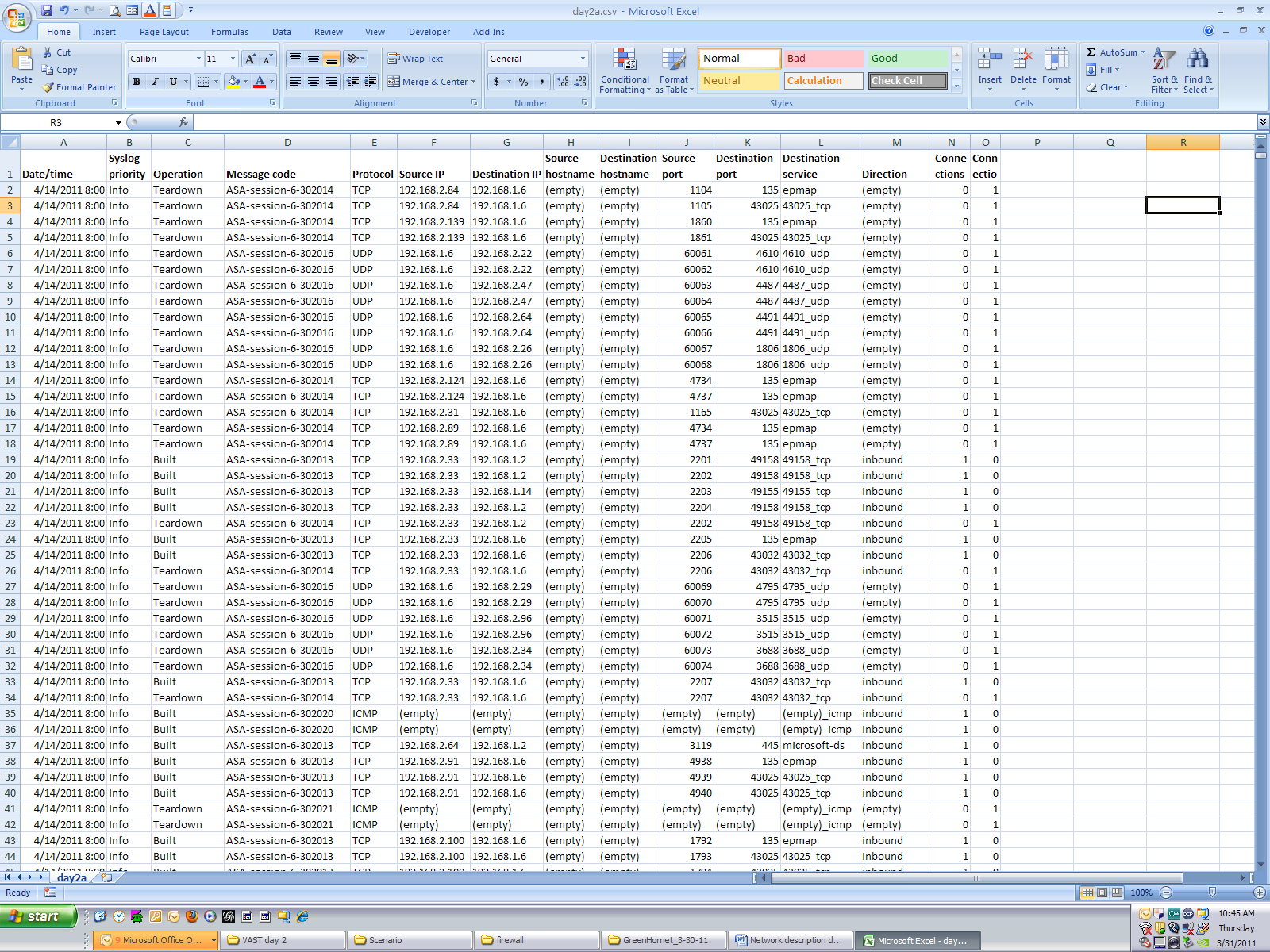


Figure . Firewall Log Excerpt

1. Intrusion Detection System (IDS) logs

The Intrusion Detection System used by All Freight is Snort.  Snort is a fully customizable IDS used to detect different types of network traffic. The system is currently configured with the following rules (the default configuration):

local.rules, bad-traffic.rules, exploit.rules, scan.rules, finger.rules, ftp.rules, telnet.rules, rpc.rules, rservices.rules, dos.rules , ddos.rules, dns.rules, tftp.rules, web-cgi.rules, web-coldfusion.rules, web-iis.rules, web-frontpage.rules, web-misc.rules, web-client.rules, web-php.rules, sql.rules, x11.rules, icmp.rules, netbios.rules, misc.rules, attack-responses.rules, oracle.rules, mysql.rules, snmp.rules, smtp.rules, imap.rules, pop2.rules, pop3.rules, nntp.rules, other-ids.rules

This dataset includes one IDS log for each day in text file (*.txt)* format that includes all intrusion detection events for the entire network for that day.

Each log entry contains many details. If opened in WordPad, as shown in Figure 2, each log entry takes up to 6 lines and is followed by a blank line before the next entry. The important parts of a log entry are identified in Table 2. Here, the line number refers to the line number of the entry shown in the WordPad example.

Table . IDS File Content

|  |  |  |
| --- | --- | --- |
| **Line #** | **Content / Format** | **Useful Content for this Challenge** |
| 1 | [\*\*]  [*Snort Rule File*]  *Text of specific rule violated*  [\*\*] | Text of specific rule violated |
| 2 | [Classification: an optional generalized description of the alert] [Priority of the alert] | Classification (if present)  Priority |
| 3 | Date/Time MM/DD-HH24:MI:SS.milliseconds  Source IP/Port  Destination IP/Port | Date/Time  Source IP/Port  Destination IP/Port |
| Remaining lines | *No content used in the challenge* | None |

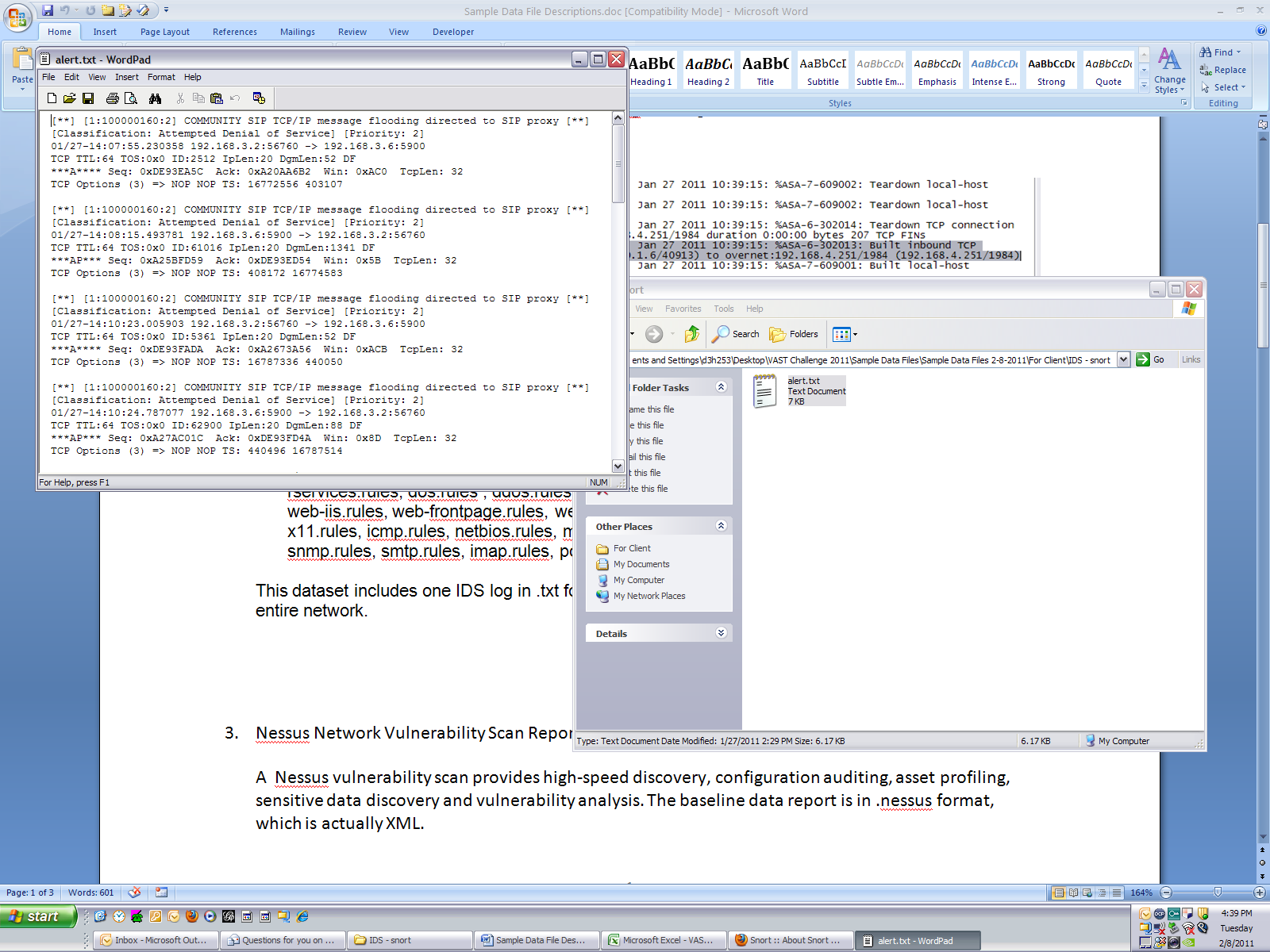


Figure . IDS alert excerpt

1. Nessus Network Vulnerability Scan Report

A Nessus vulnerability scan provides high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis. A single Nessus scan report contains the summary for the entire All Freight network. The Nessus scan provides information about the various vulnerabilities, including patch status, on the network.

The data report is provided in a Microsoft Excel file. This file was derived from the original Nessus Back End (.nbe) report. The original .nbe file is also provided.

The Nessus scan report contains the following. Line numbers refer to the lines shown in the Excel file sample in Figure 3:

* Line 1: Timestamp for the start of the scan
* Line 2: Timestamp for the start of the first IP scanned
* Lines 3-6: Results information not relevant to this challenge
* Lines 7-n: Results for specific issues found. The column values are as follows:
  + A: “results”
  + B: the subnet
  + C: The IP scanned
  + D: The port number accessed
  + E: The Plug-in ID – *this value is not used in this challenge.*
  + F: Severity level.
    - Security Hole - most severe
    - Security Warning
    - Security Note – least severe
  + G: Multi-line description of the issue or vulnerability
* Line (n+1): Timestamp for the end of the scan for the first IP
* Last line of file: Timestamp for the end of the scan.

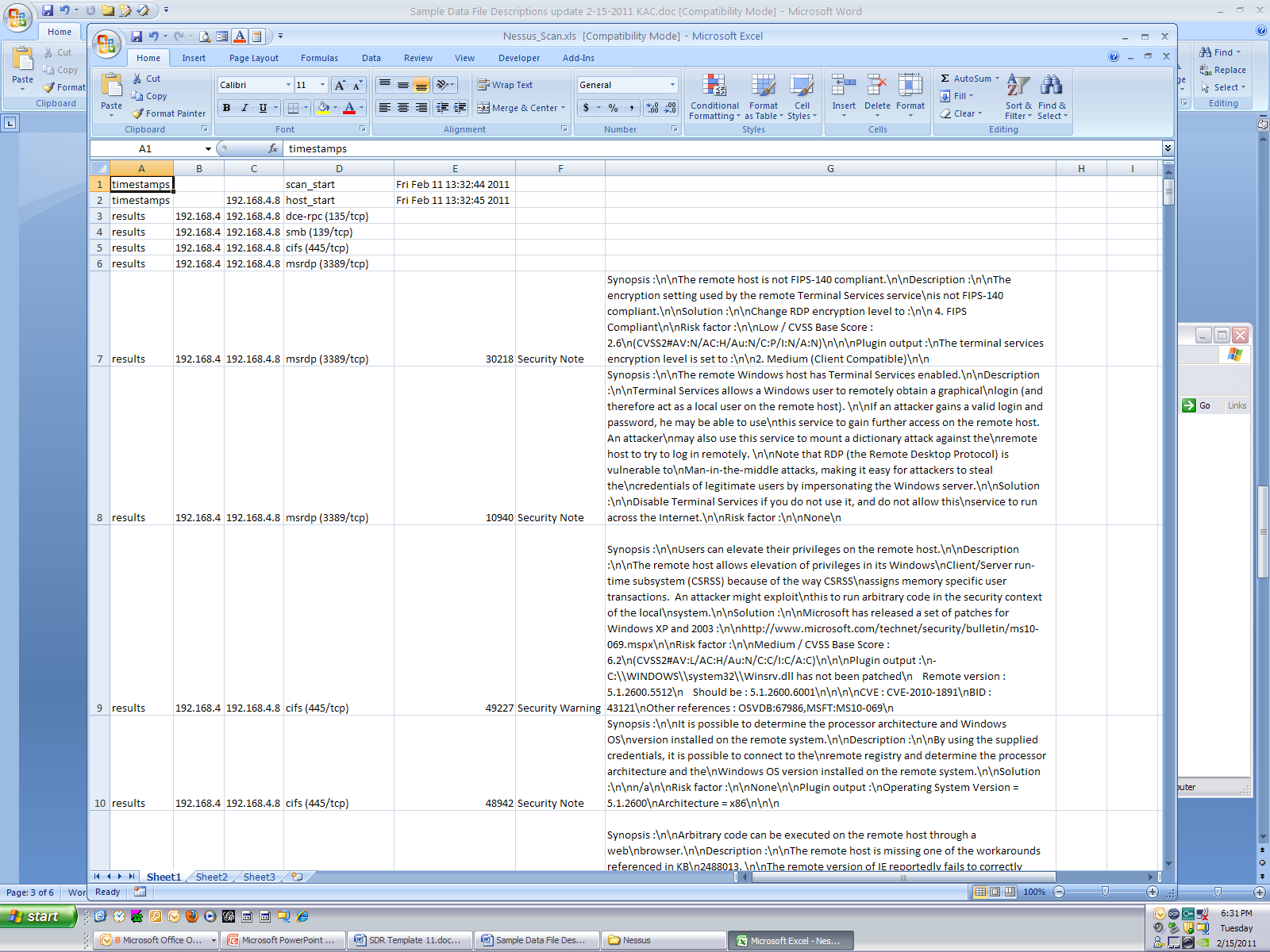


Figure . Nessus scan excerpt

1. Operating System Security Event Log

The security log from the Windows 2008 Server operating system is provided. This log has been converted to XML format. One log is provided for the entire network for each day.

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. Multiple entries may be recorded if a particular action creates multiple security events. Events are ordered in the log with the most recent at the top.

Two example log entries are shown in Figure 4. The important content of the log entries includes the following:

* EventID –indication of the type of event being logged. The full list of EventIDs and associated meanings can be found at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;947226>
* TimeCreatedSystemTime – date and time of the system event
* Data fields – Each <Data> entry contains the name of the type of data present and the value of the data. Typical values will include the username, the domain name, the IP address, the workstation name, or the port name.

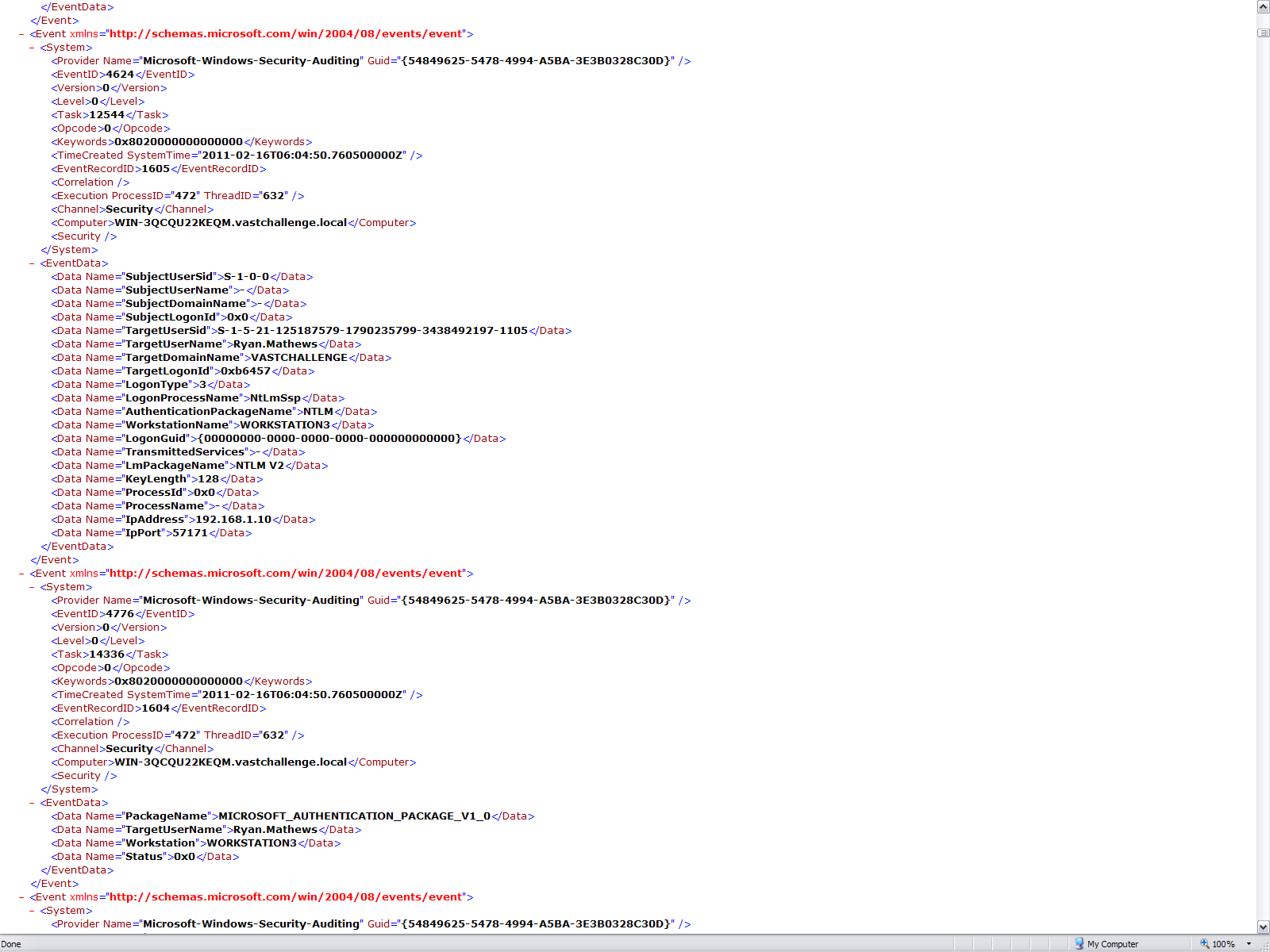


Figure . Event log excerpt

1. Packet Capture (PCAP) Log

Data from the All Freight packet capture (PCAP) logs is provided, although it is not required to solve the challenge. The PCAP data from All Freight is logged by Wireshark. A special monitor port on a Cisco switch is configured to send all packets to WireShark for packet capture and analysis.  Data is logged in multiple logs throughout the day. Individual logs correspond to specific timeframes. Due to the large size of the capture files, Wireshark was restricted to capturing only the first 40 bytes of each packet. PCAP data is being provided in its native Wireshark format. Among the PCAP contents are the following:

1. Timestamp

2. The source internet protocol (ip) address and the port used.

3. The destination ip address and the port used.

4. Protocol Type

5. Packet header information (maximum of 60 bytes per packet)

6. Packet data which shows what data is being sent over the network.

7. Network interface card information such as the manufacturer and the MAC address.

Reference used: <http://wiki.wireshark.org/Development/LibpcapFileFormat>