

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

STIPULATION OF
EXPECTED TESTIMONY

Mr. Gerald Mundy

26 June 2013

(U) It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Gerald Mundy were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. (U) I am currently a Branch Manager for the Bureau of Intelligence and Research (INR) at the Department of State (DoS). In this position, I am responsible for supervising the staff and contract personnel within INR. I am the Information Security Systems Operator (ISSO) for INR. I have worked there since 2012. Before working there, I was with Information Resource Management (IRM) at the DoS from 2006 to 2012, where I managed the contractors, the firewall program and engineering, and managed both classified and unclassified firewalls. In this position, I ensured the security of specific DoS systems used to secure CLASSNET, the internal DoS classified system, as well as Net-Centric Diplomacy (NCD). Prior to that, I was a contractor for DoS from 2002 to 2006 and did similar information technology (IT) security work. Finally, from 1982 to 1996, I served in the US Army. During this time, I was a Military Police Officer (1982 to 1984) and also worked as a 72G in telecommunications (1984 to 1996).

2. (U) In addition to my work experience, I have several certifications which qualify me for my current position. I am, for instance, a Certified Information Systems Security Professional (CISSP). This is a globally-recognized standard of achievement that confirms an individual's knowledge in the field of information security. Furthermore, I am certified as an Information Systems Manager (CISM), which trains on the information management to include capacity, planning, design, and development of systems, and Network Plus Security training, which is vendor-neutral security training, similar to what is taught in CISSP training. I have vendor training and certifications in the Stonegate software for system administration and engineering as well. Stonegate is the software used by the DoS firewall, which is made by Stonesoft.

3. (U) A firewall is a boundary which protects a computer system. The firewall in this instance protects our NCD database as well as our CLASSNET. NCD is located in what is commonly referred to as the "DMZ" between the Department of Defense's SIPRNET and DoS's CLASSNET. The "DMZ" is protected with special access. The firewall is located in the "DMZ" between SIPRNET and NCD. There is another firewall located between NCD and CLASSNET. The firewall logs track the data entering a server which exists on SIPRNET and CLASSNET. The DoS firewall software automatically registers the IP address of computers accessing our system. It further tracks the source, time and date of access, destination, action, protocol, and port associated with that IP. A log is created any time a Hypertext Transfer Protocol (HTTP) talks to a TCP and successfully receives information. An HTTP is the foundation of data communication for the World Wide Web. It consists of packets of data,

(b) (1) (B)

which, when connected wirelessly or via Ethernet cable, creates a network for communication. A TCP provides reliable, ordered, error-checked delivery of a stream of data between programs running on computers connected to the Internet. Simply put, if HTTP is a highway, TCP constitutes the lanes on the highway.

4. (U) The log data is computer generated and can be searched by network personnel who need to access the information it collects. Normally, we use this data to ensure the security of our system. I know the firewall data is accurate because it is computer-generated and it always logs. There is no possibility of error because if the system gets full it starts to overwrite the oldest information. In addition, our network personnel conduct troubleshooting on the system by interrogating the logs on a daily basis. This means we check the logs to ensure that the system is pulling data as intended and expected. The audit data is maintained on our own CLASSNET, on its own protected closed-system interface. The firewall logging software and the data it produces are, therefore, secure.

5. (U) I became involved in this case after the DoS Deputy Chief Information Officer (DCIO) Charlie Wisecarver requested that I isolate data from the firewall logs for November 2009 to June 2010 and for IP addresses 22.225.41.22 and 22.225.41.40. To execute Mr. Wisecarver's request in this case, I supervised the pulling of the information. The command used to interface with our firewall logging software is more user-friendly than Structured Query Language (SQL). The files were pulled in date and time groups because of the size of the files and were saved in .pdf format. Saving is a automatic function of the SQL-like command when entering the search query database to pull the information. The information was not altered in any way during the computer-generated pull. The information that is pulled and the format in which it is saved will vary depending on the type of command written.

6. (U) I will explain the logs by using the following example, which is an entry pulled from the file containing the date range 1 February 2010 to 1 March 2010 from the 22.225.41.40 IP address:

(b) (1)

(b) (1) (B)

(b)

(b) (1)

a. (U) If there is no information in the log, it means that there is no relevant information for the entry.

b. (U) The "Creation Time" is the time that the user was allowed through the firewall. In the above example it is "2010-02-14 15:41:38."

c. (b) (1) (B)

d. (U) The "Event" is what the user was doing. It shows the action that triggered the rule. In the above example, "New connection" is the event, which is showing that the source IP address was trying to establish a new connection with the destination IP address.

e. (U) The "Action" is what the firewall is doing. Typically, the firewall will allow or deny the event. In the above example, the action is "Allow" which means that source IP address was able to establish a new connection with the destination IP address. The user was able to enter NCD and access what the user requested.

f. (U) The "Src Address" is the source address. This is IP address of the system that is sending the request. In the above example, the source address is "22.225.41.40." This was one of the two IP addresses encompassed by our data pull.

g. (b) (1) (B)

h. (U) The "Service" is just an administrative term and represents the name of the web browsing protocol. In the above example, it is "Generic_80."

i. (U) The "IP Protocol" is the way the IP addresses are communicating. In the above example, it is "TCP" (Transmission Control Protocol). TCP is further described above.

j. (b) (1) (B)

k. (b) (1)

l. (b) (1) (B)

(b) (1) (B)

(b) (1) (B)

m. (U) In summary, the above entry tells me that the computer with the IP address 22.225.41.40 accessed the NCD server on 14 February 2010.

7. (U) Once all the firewall logs were pulled and saved onto the share drive, they were burned to a disk. I then brought the disk to the ISSO for a classification review. After the classification review, I gave the disk to Mr. Wisecarver. At no point in collecting, preserving, or transporting the information did I alter the content or device used to store it. I have no reason to believe this evidence was altered or contaminated in any way.

8. (U) A firewall is a mechanism designed to keep unauthorized IP addresses from connecting to a network or computer system that could contain a database. The DoS firewall only prevented a source IP address from outside the DoS from connecting to the CLASSNET. The firewall only regulates connections by IP address. Types of access and authorities were regulated by the NCD, if at all, once a connection was made through the firewall. There is no evidence to suggest that PFC Manning used any tools to defeat the firewall protections. Like all users on SIPRNET, he was authorized to connect using SIPRNET through the firewall to NCD.

9. (U) The log data is on a standard silver-colored CD marked with "WikiLeaks DoS Firewall Logs 13 Oct 10." I recognize the firewall log data based on the date and time stamp of the logs, as well as the information type pulled and the nomenclature such as the vender marks and the initials "IPS, FW" that appear at the top of the logs, which signify the DoS bureau and firewall. Through my work I have experience reading these types of logs. And, in this case, I pulled a sample of the requested information to ensure it was what DCIO Wisecarver wanted.

Prosecution Exhibit 108 for Identification is the log data I pulled.

//ORIGINAL SIGNED//
ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel

//ORIGINAL SIGNED//
THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel

//ORIGINAL SIGNED//
BRADLEY E. MANNING
PFC, USA
Accused

(b) (1)