Corporate Espionage Scenario

The following is an introduction letter that will be given on Monday evening to the students. At that time we will ask them to assist us in investigating the scenario.

Overview
As the Corporate Security Officer for the Nethken Corporation, my team and I are responsible for the overall direction of all security functions associated with Information Technology applications, communications (voice and data), and computing services within the enterprise. We are also responsible for the physical security, protection services, and privacy of the corporation and its employees. Through this role I coordinate security efforts across the enterprise, including information technology, human resources, communications, legal, facilities management, and other groups to identify security initiatives and standards.

As background, our company is a 9-to-5 operation; that is, the entire building is empty every night with the exception of our physical security staff stationed outside and a few janitors inside (that clean the bathrooms, vacuum the carpets, empty all the trash cans, and so on). Nethken Corporation makes a good deal of money doing what we do and are very good at it. We have competitors that might want to know the details of current projects and upcoming products in order to launch their own competing versions. Currently, our company is at the end of a major development cycle of a new design that we plan to announce next Monday. Needless to say tensions have been high as Monday approaches. Over the last several days my team and I have been begun to suspect that one of our own employees may be attempting to exfiltrate information about our latest design to one of our competitors. Because of time sensitivity and our announcement being next Monday, I am requesting your assistance in determining if our beliefs that an insider is divulging confidential information to an outside source are correct.

We have obtained some relevant information through a preliminary analysis of the situation and a sweep of our building. We need your help to answer the following questions:

(1) Who is the employee (the insider) exfiltrating our intellectual property (IP)?
(2) How did s/he exfiltrate our IP?
(3) Who was the target/outsider (the receiver of the IP), and who does s/he work for?
(4) What IP did the insider exfiltrate?
(5) How should we (Nethken Corporation) respond as a company?

Preliminary Evidence
We have been able to narrow down the location of the insider threat to a shared office within our building. This office is large and is populated by as many as 25 employees in its cubicles. A thorough sweep of the shared office space was performed this morning by our security team before any employee arrived and after all janitors had left the building. Some suspicious items were identified:

(1) A locked box was found hidden behind a flower vase on top of a filing cabinet in the corner of the room.
(2) Shreds of paper were found in a garbage can.

Internal note: The locked box is opened with a 3-digit code (248). This code is significant in that it represents a room number in Nethken Hall that the students will need to enter later on (with the magnetic card) to obtain a password (for the steg document) written on a post-it note on a desk (and as

an impression on the top sheet of a pad of paper), a hard drive (a clone of a hard drive in one of the machines the insider uses to communicate with the outsider), and a “readme” for the steg tool (used to extract the steg document later). The box contains a “readme” document for network traffic sniffing tools and a magnetic card used to open the room.

The shreds of paper form a single document that identifies a password (for the steg document). The password can also be obtained in Nethken Hall 248 on the post-it note.

On Tuesday morning, the students will be given a network dump on a USB stick. They will be told that this dump was obtained after the preliminary analysis by an analyst who was able to find cached information on a server that handles Nethken Corporation's incoming and outgoing network traffic. The dump will contain a variety of useful information (along with plenty of white noise):

(1) The insider's name and an associated IP address.
(2) The outsider's name and an associated IP address.
(3) The name of the company the outsider works for.
(4) The name of the building and room number the insider has been using (in addition to the shared office space) to communicate with the outsider (NH 248).
(5) A web page frequently visited by the insider. This web page is a means of communicating the current password for a wireless network used by the insider and outsider to communicate.
(6) The SSID to this wireless network.

With the information from the investigative session (covering networking basics and network security), the students will be able to analyze the network traffic dump for this information.

On Tuesday afternoon, the students will be given an email (with headers) containing the following information:

(1) The building name (Nethken Hall)
(2) The room number (248)
(3) The insider's IP address (in the header)
(4) The outsider's IP address (in the header)

They will be told that it was obtained recently (after enlisting the students' help). Note that NH 248 will have a sign posted on the door that it is only accessible on Wednesday, so teams that discover the room number ahead of time won't be able to get in yet.

On Wednesday morning, the students will be given an Android phone. They will be told that it was found on the floor behind the filing cabinet in the shared office space after a second sweep was done. The phone contains the insider's name and a Google map with a GPS location identified on it. This location points to a foam rock located on campus with an encrypted message (artichoke) underneath it. This message identifies the web page frequently visited by the insider.

With the information from the investigative session (covering cryptography, physical security, and hard disk analysis), the students will be able to decrypt the message under the rock, locate the room the insider has been using to communicate with the outsider (NH 248), obtain a password (for the steg document), obtain a hard drive image of the insider's computer system located in the room, obtain a “readme” for the steg tool, and be able to analyze the hard drive image.

The hard drive image will contain a variety of useful information (along with plenty of white noise):

(1) An email that contains the SSID and password to a wireless network the insider uses to communicate with the outsider.
(2) Facebook and Twitter accounts the insider uses.
(3) The IP addresses of the insider and outsider.
(4) An image that seems suspicious (it contains a steg document – a portion of the grand prize design document). This image is also on the insider's Facebook page.

Internal note: The web site obtained by analyzing the hard drive image, analyzing the network traffic dump, and located in the encrypted message under the rock, requests an SSID as input. Upon being submitted the correct SSID (obtained via the email on the hard drive image or in the network traffic dump), it will provide an encrypted phrase (artichoke) containing the password to the wireless network.

The Facebook and Twitter accounts also contain the outsider's name and company. Moreover, the Facebook account contains the same image that contains the steg document (and is also obtained on the hard drive image).

On Thursday, with the information from the investigative session (covering steganography, advanced network security, and wireless networking basics), the students will be able to obtain access to the wireless network used by the insider and outsider, and sniff "live" network traffic on the wireless network to obtain the entire IP the insider exfiltrated. This is the grand prize. In the end, the students will be able to provide the insider's name, the outsider's name and company, the method the insider used to exfiltrate the confidential intellectual property, and formulate a response and course of action.

Internal note: The steg document is a teaser document that was exfiltrated to the outsider as proof that it could deliver the "goods" (the full IP document which is the grand prize).

Tuesday's daily scenario should be representative of the following investigative topics:

(1) Networking basics
(2) Broad network security issues (denial of service, man-in-the-middle)

Wednesday's daily scenario should be representative of the following investigative topics:

(1) Physical security
(2) Basic cryptography (artichoke)
(3) Hard drive image analysis basics
(4) Forensics investigation basics

Thursday's daily scenario should be representative of the following investigative topics:

(1) Steganography basics
(2) Wireless network basics
(3) Basic wireless network security issues (SSID hiding, MAC filtering, WEP encryption)

Friday's 24-hour scenario can make use of all the previous days' investigative topics. Note that the optional investigative session on this day can be a rehash of the previous days' content. An option is to let the teams know that, in this final investigative session, they have 45 minutes as a large group to ask

as many questions as they wish. Subsequently, we will have personal team time, where several of us will go around to each team and allow them 45 minutes to ask a number of questions personally (i.e., without the other teams knowing).

Required equipment/content:

(1) Laptop with network sniffing and steg tools
(2) Locked box (with the lock code 248)
    (a) Readme document for network traffic sniffing tools
    (b) Blank magnetic access card
(3) Shredded document containing the steg document password (this can be a simple handwritten note on a sheet of paper noting a description of the image the steg document is hidden in and its password)
(4) USB stick with a network dump; packets should contain emails (some with text attachments), chats, and so on that identify:
    (a) The insider's name and IP address
    (b) The outsider's name, company name, and IP address
    (c) The lab the insider has been using (NH 248)
    (d) The web page URL frequently visited by the insider
    (e) The SSID to the wireless network the insider uses to communicate with the outsider
(5) A note on NH 248 noting that it is only open on Wednesday
(6) An email (with headers) containing the building and room location (Nethken Hall 248), the insider's IP address, and the outsider's IP address (the latter two in the email's header)
(7) Android phone
    (a) The insider's name should be prominent
    (b) A Google map with a pin identifying a foam rock somewhere on campus
(8) Foam rock with an encrypted message underneath it located somewhere on campus
    (a) The message should provide the web page URL frequently visited by the insider
(9) A “fake” computer on a desk in NH 248
    (a) A post-it on the desk (underneath the keyboard) with the steg document password
    (b) A pad of paper with a pen; its top sheet should reflect an impression of the steg document password
    (c) Readme document for the steg tool
(10) USB stick with a hard drive image
    (a) Email containing the wireless network SSID and password
    (b) Facebook account (with image containing the steg document)
    (c) Twitter account
    (d) The insider's IP address
    (e) The outsider's IP address
    (f) An image (seemingly suspicious) that contains the hidden steg document
(11) An image with a hidden document
    (a) The hidden document is a teaser of what IP the insider has been exfiltrating to the outsider
(12) Web site that accepts the SSID and returns the WEP password (encrypted in a phrase)
(13) Facebook account
    (a) The outsider's name and company
    (b) An image (seemingly suspicious) that contains the hidden steg document
(14) Twitter account
    (a) The outsider's name and company
(15) Wireless network router

(a) A script that generates “real-time” “live” network traffic, some of which represents insider-outsider communication
(b) Some of the traffic needs to represent exfiltration of the IP from insider to outsider
(c) The wireless network should be encrypted using WEP

The following is a graphical view of the scenario. Blue represents items “given” to the students, yellow represents transition items (such as locations or objects), and red represents items the students have to obtain or figure out. Note that every red object should be obtainable via two or more methods in case a group misses something.