AbOSE Public Report

- Version 1.0
- file: <abose- public- 2006feb03.doc>
- date: 2006 Feb 03
- author: T. Charles Yun <tcyun@internet2.edu>

TABLE OF CONTENTS

Introduction

On Tuesday 29 November 2005, the first Abilene Operational Security Exercise (AbOSE) was held on the IUPUI campus in Indianapolis, Indiana. Eight individuals from the Network Operation Center (NOC) from both the service desk and the engineering team were assembled to discuss typical activities, documentation and complete two "table top" scenarios.

It is important to note that this exercise was not an audit. This fact was mentioned to the participants and the timber of the exercise was designed to be casual and conversational. The goal for the first exercise was to gather the correct individuals in one room and begin the relevant conversations.

This document is a summary of the official exercise report. Sensitive details have been removed but the overall understanding and value of the exercise should be evident. The official exercise report lists a set of observations and recommendations for the NOC; these observations and recommended responses will form the basis for follow up exercises. If you are interested in learning more of the details of the exercise, please contact T. Charles Yun or a member of the Abilene Network team at Internet2.

While activities to improve the effectiveness and responsiveness of the participating organizations will continue through other channels, this document marks the successful end of the first Abilene Operational Security Exercise. Internet2, the Abilene team and the Internet2 community at large would like to congratulate the NOC on their performance and thank the individual participants for providing their time and energy.

T. Charles Yun, 2006 Feb

(on behalf of Internet2, the Abilene Team, and the Internet2 Security Team)

Exercise Format

The Abilene Operational Security Exercise (AbOSE) was a one day long event designed to initiate conversations on the Network Operation Center's (NOC) activities in their support of Abilene, Internet2's national, backbone network. The need for this type of exercise has been generally acknowledged and understood since the inception of Abilene and the NOC. Typical constraints to time and schedule delayed executing this event. Recently, a series of high profile events as well as a general increase in the importance of security response across the community as a whole helped to make the exercise a reality.

In developing the exercise, two groups were created: organizers and participants. The organizers created the scenarios and narrated the exercise. The organizers also held responsibility for administrative concerns such as communication, room logistics, note taking, etc. Internet2 took the lead as organizer, with significant technical assistance from a NOC engineer and important administrative assistance from the IUPUI location.

The participants' responsibilities were restricted to the day of the event. A decision was made during the planning of the exercise to keep detailed information regarding the security scenarios away from the participants so that reactions to the events would be realistic.

Participants for the exercise were determined by asking managers from the participating organizations to identify a group of individuals representative of the team who would be involved

in a security incident. The individuals came from the NOC, Indiana University, the REN-ISAC and Internet2.

The day of the exercise can be divided into three sections. The first section covered general introductions, individual's responsibilities, documentation and communication. The second and third sections were tabletop exercises designed to be realistic and require interaction with a wide variety of groups.

The security scenarios for the second and third sections were developed from a large initial list gathered via suggestions from individuals familiar with the NOC and networking. From the large list, two scenarios were selected and refined.

Analysis: Exercise

It is important to note that Intenret2 has a great deal of confidence in the NOC. Historically, the NOC team has been professional, competent and responsive. Interaction with the NOC team during the exercise also reinforced these beliefs.

As mentioned, this exercise was not an audit. Therefore, explicit and detailed investigations of specific processes were not pursued. Instead, the two scenarios were designed to explore difficult technical problems that would indicate how processes were implemented and followed.

During each scenario, the organizers and the participants both noted the limitations of the tabletop format. For example, participants were not given a clear understanding of how their actions and conversations in the room corresponded to the execution of activities in the imagined time of the scenario. Further, activities that would occur in parallel by multiple participants were often pursued serially during the scenario. During the second scenario, a turn based system was implemented and improved the interactions. This concept should be refined in future activities.

In another example, participants stated that they received responses to some of their actions indicating that the activity was fruitless. Organizers either provided poor feedback or misunderstood the purpose of the participants' activities. In the future, an explicit process for each "turn" should be enforced: open discussion, formal statement of activity by participant, formal response by organizers, clarification, next turn.

A related issue was noticed regarding the serial nature of the conversations. There was a tendency for one individual to take over conversation for an extended period. The organizers should determine if this is because individuals act as "ticket leaders" (the most active individual responding to the ticket) or if this is an artifact of the format.

An inherent limitation of the tabletop format is the inability to predict the information participants will request. Matt Davy provided a great deal of background during the planning stages. During the scenarios, he provided information based on his experience and access to other engineers who were available via instant messaging. In spite of this, the participants felt that the experience would have been more realistic if actual test reports could have been run (or presented). The combination of Davy and the remote engineer's expertise worked extremely well for the exercise, but a more robust process should be investigated.

The organizers also received feedback indicating that our use of "actors" could have been expanded to include the NOC's clients. The organizers asked Internet2 staff to play the role of a reporter. This interaction, while short, was interesting in that it added additional free-form information into the exercise. Having an actor on hand to play the NOC's client would have been interesting, particularly to raise the urgency of the scenario in real time. The limitations to additional actors are primarily time based.

Another point of feedback to the organizers was a critique of the scenarios. There was a concern that the scenarios tested the cleverness of engineers, not focusing on process. Noting that the goal was to investigate activities and not audit process, the organizers acknowledge that the exercise seemed to focus on the ability to respond to technical issues. The organizers feel that the response to these technical issues revealed a great deal about the NOC's process. Future exercises should investigate if the technical focus is the most effective angle into the NOC's processes and procedures.

Scenario 1 Analysis

The first scenario was described to the participants using the below text:

> Assume that an important demo has been in the works for several months. As expected, the NOC has been participating (altering routes, looking at netflow data, etc.) in support of the users. The demo set up and testing took a while, but everything is working now, and you are all quite happy with things. The demo-ers just called to say that they were starting to relax as the last test just completed and the actual demo will begin at 2pm today.
>
> This is an important demo because a group of researchers are coming together to pitch to a funding organization. If the demo goes well, the funding is expected to start immediately. However, there are some concerns about the reality (even at the demo stage) of the technology and the funders have been expectations managed... to expect that this is going to be a fancy and impressive demo.
>
> The application consists of two parts. The first part is a series of three, uncompressed video streams that have been sampled in such a way that each video signal requires 1.5 Gbps. Two streams are parts of a 3D image and must be tightly synchronized. The third video stream is video display of a talking head. All three streams are sensitive to loss and jitter. Loss/jitter over .05% is noticeable and the streams becomes unusable at 1.5%.
>
> The second part is a smaller data stream of up to 500 Mbps is also being sent. This stream consists of real time data from the results of an experiment. Results are continuously produced, but at varying rates. This stream can sustain loss/jitter rates of up to 10%.
>
> In addition to the two "experimental" parts, the demo has a backup H.323 connection.
>
> Thus, the total bandwidth required for the experiment is ~5 Gbps:
>
> 3 @ 1,500 Mbps
>
> 1 @ 500 Mbps
>
> 1 @ 2 Mbps
>
> The flow will start on the east coast, travel over the backbone to the west coast. From the backbone egress point on the west coast, it will head to the final location over regional networks.

Once the background was provided, the exercise started with the following statement:

> It is noon the day of the demo. For some reason, the video link has started to see some choppiness. It occurred twice in a ~20 minute period and the demo-ers have asked to see if anything has been changed. They have done extensive monitoring and troubleshooting on their side and do not believe the problem is at the end hosts.

The above text was treated as if it were a call into the NOC. The question was handed to the individual who would have answered the NOC phone and the entire exercise was started.

The first exercise was run for about 2 hours and required the interaction from most areas of the NOC (ticketing, engineering, etc.).

General Observations

The problem ticket process seems well thought out and was consistently executed for both scenarios. It is difficult to gauge how well the community understands how and when to contact the NOC. However, once the NOC establishes contact, the ticketing and triage process begins. The service desk was observed requesting specific information regarding the problem and request/confirmation of contact information.

Once triaged, engineers seem to be contacted quickly. Information sharing includes data obtained via Service Desk script.

Engineers began working on the problem and attempted to determine the severity of the situation. (Note, the participants assumed that the severity of this scenario would be high due to the nature of the exercise, but the participants walked through the initial steps as if they were not yet certain.) Engineers began pursuing a large variety of sensible and rational tests. While these tests were completed quickly, the engineers did not seem to be following a template nor was a checklist observed.

External parties were integrated into the scenario. This includes external parties who contacted the service desk (e.g., REN-ISAC) and parties that the NOC contacted (e.g., Cotter/Corbato/Summerhill).

Due to the design of the scenario, the user was not represented. It was noted that a real event would probably have included more interaction with the user.

After the scenario was completed, the organizers and participants held a short debriefing session. The conversation indicated that some type of report would be sent out to the affected parties and potentially the community at large. The post-incident process should be explored.

Scenario 2 Analysis

The first scenario was described to the participants using the below text:

> RPD process restarts on a backbone router.

Once the background was provided, the exercise started. The assumption is that one of the engineers would have received some indication that the process was restarted.

General Observations

As with Scenario 1, the Service Desk process is executed effectively. Note that in this scenario, the ticket is generated internally by the NOC. Service Desk runs triage: contacts engineers, confirms issue and establishes initial severity level. Ticket is passed to an engineer and work begins.

Similar to the previous scenario, engineers executed a series of tests based on experience, but did not follow a checklist. During the scenario, it became evident that a root level router compromise had taken place. In the case of a root level compromise, one would expect an in place procedure that regained/established control of all NOC machines. Note, however that due to miscommunications during the exercise, the organizers were

attempting to conceal the full extent of the compromise and participants might have understood the obfuscation to be an indication that there was no need to move further investigate.

As part of the exercise, the process by which the machine was prepared for offline forensic analysis was discussed; this activity should happen in “real life” as a high priority activity. A SANS document was mentioned regarding forensic steps/preparation, but actions were not referenced against the document.

Once engineering completed initial investigations, escalation occurs. Escalation to NOC personnel, Abilene, local IT staff, REN-ISAC and vendor proceed. Note that IT staff contact occurs via email and response time is not guaranteed. The uncertainty in response time should be acknowledged and addressed, but quickly followed by the fact that the IT staff office is across the hall from the NOC.

As part of the scenario, an Internet2 staff member posed as a reporter. The participants understood that they were not to respond to the reporter directly. It was noted that the need to push the reporter to Internet2's media relations group was obvious due to the nature of the exercise. Additionally, the reporter posed an initial question that made it obvious that he was attempting to obtain information regarding the scenario. Herron noted that if the reporter had led with a series of general questions, NOC personnel might have responded politely for several questions before realizing the situation. There is a tension between politeness and strict policy adherence.

Next Steps

The Abilene Operational Security Exercise was initiated as a first step in an ongoing process. Based on the information collected and initial suggestions outlined in this document, it seems appropriate to suggest follow up activities. In the near term (0-3 months), the NOC should address issues raised in this document and integrate the changes and improvements they feel necessary. In the mid term (3-6 months), Internet2 should present the NOC with a plan for a second Abilene Operational Exercise. For the ongoing future, the NOC and Internet2 should agree upon a schedule that encourages constant analysis and improvement through a regularly scheduled set of exercises.

Looking beyond Abilene to the research and educational networking community as a whole, Internet2 believes that cross network coordination between NOC's should be investigated. To that end, Internet2 is working to schedule similar operational exercises with national and international networks.

Time Frame	Description
0-1 months	Internet2 collaboratively develops plan for second AbOSE
2 months	Internet2 announces schedule for second AbOSE
0-3 months	Internet2 collaborative develops plan for multi-network exercise
0-3 months	NOC addresses issues from AbOSE report
4-5 months	Second AbOSE executed

Table 1: Timeline for AbOSE Next Steps

Conclusion

The Abilene Operational Security exercise provided an opportunity to share information, experience NOC processes and determine if major gaps existed. Overall, the NOC team

displayed professional, competent and effective in their response to a pair of scenarios designed to be complex and out of the ordinary. No major gaps in process were observed, however, several problems were noted.

This document serves to summarize Internet2's observations of the exercise. We encourage the NOC to identify any points of disagreement and present those items with their reasoning back to Internet2. Internet2 assumes that obvious areas of improvement noted in this document will be addressed.

To maintain an ongoing environment of improvement, Internet2 proposes a schedule to run a more rigorous exercise that will follow up on the first AbOSE as well as investigate other areas of the NOC's activity.