Cooperation---The Foundation of Network Security

It has happened again. A user has just called to complain about the network being slow. As the building network administrator on a university campus, you have received calls like this intermittently over the past two weeks. Previous periods of network slowness were of short duration limiting your ability to match it to any specific cause. But today you discover, through the use of the web tools provided by the university Information Technology Department, that all the users share the same LAN segment and you see that the bandwidth utilization on that segment is spiking to near 100%. Since the baseline bandwidth utilization on this segment is under 10%, further analysis is warranted.

In cooperation with the Information Technology Department, a port is identified as the source of the increased bandwidth usage. According to university policy[1], the port is disabled until the device that appears to be generating the network traffic can be secured. When the network administrator looks at the UNIX workstation using the port, it is discovered that a log file exists that has been capturing usernames and passwords from the network traffic on this shared Ethernet segment.

Before this incident can be closed, there will be hours of:

- contacting **users** to secure accounts,
- **system/network administrators** gathering data from system logs,
- messages and phone calls to technical and administrative contacts of **other sites,** both national and international,
- meetings with and supplying data to **law enforcement agencies**, in this case, the campus police and the FBI,
- contacting operating system v**endors** for security patches,
- seeking guidance from the Legal Counsel's Office,
- filing reports with the **network security organizations** at the university and others, like the Computer Emergency Response Team (**CERT**)[2],
- contacting the System Administration, Networking, and Security Institute **(SANS)[3]** to learn about the compromise and how to recover from it,
- and interaction with your **management** to keep them apprised of the situation.

During each of these interactions cooperation was a key component. Let's explore the motivation for the cooperation between and among folks as this incident-handling process was brought to closure. We will concentrate on the points of cooperation as they took place in solving the slow network incident and the motivation that improved the probability of cooperation. Please keep in mind that this particular network security incident has taken place in the culture of a public university campus. We are focusing on the interactions between people and groups rather than the handling of the incident.

[1] Arizona State University Information Technology. " ASU Computer, Internet, and Electronic, Communications Policy" Section VI. Violations and Enforcement, Subsection E. 9 Sep 2000 URL: http://www.asu.edu/it/fyi/policies/acceptableuse.html
[2] http://www.cert.org
[3] http://www.sans.org/

Since we are looking at the intersections of cooperation, let's examine the definition of the word. What is cooperation? Webster's dictionary defines cooperation, in part, as "the association of a number of people in an enterprise, the benefits or profits of which are shared by all the members"[4]. One could define the Internet as an enterprise. All who take the adventure of using or connecting to the Internet assume or share the associated risks. When all of the devices one must traverse to get from point A to point B on the Internet are working correctly, the person seeking information benefits from finding the data and the provider has the satisfaction of making the transaction possible. Often that satisfaction is in the form of payment.

A knowledgeable network security professional understands that the risks associated with Internet use can be reduced through cooperation. Cooperation is mainly voluntary and must be fostered. It has been strengthened with policies, directives, collaborations, and, when a crime is involved, with laws. For the successful resolution of a network security incident, cooperation in the form of collaboration, interaction, teamwork, conformity, and/or compliance must take place. The network security professional must develop relationships with as many folks as needed to bring a security incident to closure.

Since everyone connected to the Internet shares in the risk associated with its use, it would benefit all to cooperate in reducing those risks and resolving incidents. Is there anything that compels others to cooperate with another's desire to find the source of a network security violation and eliminate it? The answer is yes! Another site's risk could very well become the future cause of loss of network access for you. The following will explain some of the work that has been done to put down some ground rules for Internet etiquette when dealing with folks outside your business authority. It is much like the cooperation that takes place between and among law enforcement agencies, whether local, state, national, or international, to solve a crime. There must be agreement and a desire to cooperate.

Early in the development of the Internet, it was understood that rules of etiquette were necessary for everyone to be able to use the shared resources of the Internet. Recommendations for cooperation were laid out in Requests For Comment (RFC). Although cooperation is voluntary and usually unenforceable, it is essential for the secure operation of the Internet as stated in RFC 1281.

> The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations. This assistance may include tracing connections, tracking violators and assisting law enforcement efforts[5].

[4] **Webster's New twentieth Century Dictionary Unabridged. 1972 by Simon & Schuster**

[5] RFC 1281 Guidelines for the Secure Operation of the Internet.
Http://faith.csc.twu.ca/~dfriesen/rfc1281.html

This RFC spells out the responsibilities that the university assumed when it made a connection to the Internet. It also hints at what is expected from system administrators who would have access to logs that would assist in tracing connections and tracking violators. Since not all responsibilities on the part of other players in the resolution of this incident are defined in RFCs, other forms of collaboration have been implemented as needed. Let's look at the motivation for others to cooperate as we close out this incident.

USERS
The contact from the user regarding a possible problem with the network has begun the network security incident handling process. In this instance, the network administrator has provided the users with training and the correct procedures to follow when a problem is detected with the network. The user has voluntarily followed the guidelines and reported the problem to the designated network administrator. The user is motivated by an expectation of the restoration of an efficient network. Cooperation has begun to take place.

The user, a graduate student, and the network administrator both can benefit from the network returning to normal status. Because of the shared desire that the network return to an efficient and reliable medium for the use of faculty, staff, and students to carry out the teaching and research of the university, the user and network administrator worked together toward that goal. Since the LAN segment involved in this incident is attached to the university network backbone and that in turn is connected to the Internet, the enterprise that will benefit from alleviating the cause of the network slowness has been greatly expanded.

There are no laws mandating cooperation, but compliance is requested via university, Board of Regents, State of Arizona, and global policies, RFCs and directives from management. For the documents that delineate the policies to be effective, everyone, from the local user to the leaders of countries, must be made aware of their content and encouraged to abide by them. Education and training of users is the responsibility of all network security professionals.

The user, in this case, has learned through his membership in a College department, that he should report network issues to the local network administrator. This duty is included in the local department's policies and provided to all faculty, staff, and students when joining the department. These policies are a supplement to the university, Board of Regents, and State policies covering the use of computers on the shared network university infrastructure.

SYSTEM/NETWORK ADMINISTRATOR
The network administrator, as a member of the university network administrators committee and a network security professional, maintains a close relationship with other system/network administrators and the central Information Technology department; keeps abreast of the university policies relating to network etiquette; and subscribes to distribution lists to receive advisories from vendors and the latest network vulnerabilities and solutions from organizations like CERT, FBI, and SANS.

The network administrator found that there was a file on a computer in the affected LAN segment that contained usernames and passwords that were sniffed from the TCP/IP traffic. Because other users on the shared LAN segment could benefit from knowing that their accounts had been compromised, the network administrator proceeded to notify all involved. In the spirit of cooperation, each system administrator of a university server with compromised accounts was contacted.

After checking their own systems for signs of compromise, the system administrators made telephone contact with the users to have them change their passwords. Those users who could not be reached by telephone had their accounts disabled until contact could be made. The authority to lock a user out of an account under these circumstances is presented in the university policy under Violations and Enforcement[6]. All will benefit from having a secure system.

NETWORK SECURITY ORGANIZATIONS

The network administrator reported the incident to CERT and an incident number was obtained. All communications with other system/network administrators on and off campus included the CERT incident number. The CERT incident number was used to encourage those being contacted to comply with requests for assistance in handling the incident. Reporting incidents to CERT is not required, nor does law mandate it. But the local university policy recommends it.

As each system administrators was notified of their vulnerability created by the unauthorized knowledge of account information , reference was made to web pages at SANS that explained the original account compromise with information on how to recognize it and recover from it. Other steps that could be taken to prevent future attacks were also pointed out for each operating system. CERT and SANS are each not-for-profit organizations that request cooperation from the Internet community to share information regarding network security incidents, vulnerabilities, and best practices. For everyone to benefit, the network security professional must participate in sharing the knowledge gained from handling network security incidents.

OTHER COMPUTER INCIDENT RESPONSE TEAMS

For computers off campus, the network administrator contacted the registered technical and/or administrative contacts in the WHOIS[7] database to either alert them to possible account compromises or to request assistance in locating the perpetrator and gathering information regarding the incident from their end. Most of the sites contacted had a Computer Incident Response Teams (CIRT) in place to handle this incident. These sites

[6] Arizona State University Information Technology. "ASU Computer, Internet, and Electronic Communications Policy", Section VI.Violations and Enforcement, E. 9 Sep 2000. URL: http://www.asu.edu/it/fyi/policies/acceptableuse.html

[7] RFC 954. Harrenstien, K., Stahl , M., and Feinler, E. "NICNAME/WHOIS". Oct 1985. URL: http://rfc.asuka.net/rfc/rfc954.html

understood that "Resolving these incidents will require cooperation between individual sites and CSIRTs, and between CSIRTs" as stated in RFC 2350.[8]

The locally compromised system produced information regarding the source IP numbers of the latest connections for the unauthorized account access. Contact was made with the network administrators of three possible source locations of the hacker activity. Two of the remote user accounts were disabled as a result of this contact regarding this incident. The third IP number was under the authority of an Asian country and no response was ever received from the documented contacts. Two out of three locations demonstrated cooperation. The third location was to be handled by the FBI and the legal entities of that Asian country.

LEGAL ENFORCEMENT AGENCIES

Because there was use of a computer account without the authorization of the account owner, a possible crime of fraud was involved[9]. The campus Department of Public Safety (DPS) and the General Counsel's Office were contacted and reports filed with them. All documentation relating to proof of times and sources of unauthorized access to the university computer was shared with DPS and ultimately the FBI. Without the involvement of the legal authorities, the network administrator would have no means of tracking and possibly bringing the perpetrators to justice, if that is the management's desire. The entire Internet community could benefit from bringing the perpetrator to justice.

VENDORS

The systems that were comprised and had sniffing software installed were all SGI computers running a vulnerable version of IRIX. In this instance, this was a known vulnerability. Each system administrator downloaded and installed the latest security patches provided by SGI. Most of the providers of popular operating system, software applications, and hardware provide patches freely to their customers and make them easily accessible. If this had been a new vulnerability, cooperation would have been requested from the vendor to provide a patch to close up the vulnerability as quickly as possible. The vendor would benefit from cooperating by retaining a positive reputation.

OTHER COOPERATIVE INITIATIVES

In the book, Take Down[10], the tracking of the activities of Kevin Mitnick was impeded many times by the lack of cooperation. As in any network security incident handling, progress can halt with any party's refusal to cooperation. Many of the organizations involved in the tracking of Kevin Mitnick have since developed initiatives that will foster the sharing of information about network threats and coordinate efforts to attain a more

[8] Brownlee, N. and Guttman, E. RFC 2350. "Expectations for Computer Security Incident Response". Jun 1998. URL: http://www.theinternetbook.net/RFC/rfc2350.html

[9] Arizona Revised Statutes 13-2316, Computer Tampering; venue; forfeiture; classification.

[10] Shimomura, Tsutomu and Markoff, John. Take Down. New York: Hyperion, 1996.

reliable shared Internet resource. Each of these initiatives is based on cooperation among its members for the benefit of all.

The FBI has begun an outreach program whereby it will serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. This initiative was begun under a mandate in Presidential Decision Directive 63[11] and is intended to foster cooperation among many different entities in government and the private sector in sharing information about vulnerability and threats to our critical network infrastructures.[12] The FBI cannot accomplish their mission alone. It requires the coordinated efforts of federal, state, and local agencies. Because the FBI has unique access to foreign intelligence and law enforcement information, it is the agency chosen to coordinate this effort.

Similar cooperative efforts are developing in Europe under the European CSIRT (Computer Security Incident Response Teams)[13]. Its purpose is to encourage and support the cooperation between CSIRTs in Europe. It is becoming evident to countries as more business transactions and resources are moved to the Internet, that some agreements to its use must be formalized locally and internationally.

The Center for Internet Security[14] is a not-for-profit cooperative effort to establish global best practices for businesses, educational institutions, and government entities in the United States. Its founding members have a mission to help organizations reduce the risks associated with Internet-connected equipment use. A similar collaboration was formed as a working group of the Committee on Institutional Cooperation (CIC), a twelve-university collaboration founded in 1958 and located in Champaign, Illinois. The Security Working Group is charged with developing procedures and practices that will ensure cooperation among the member institutions while investigating security incidents.[15]

As a network security professional, you can play an important role in the war against Internet attacks. This battle involves perpetrators with mechanisms in place for cooperation and, it would seem, an unlimited arsenal of weapons. You must not go into this battle as a lonely soldier. Develop your own arsenal through cooperation with all those mentioned above---the users, other system/network administrators, CIRTs, network security organizations, legal enforcement agencies, vendors, and your management. Foster relationships, educate and inform users and management of policies and procedures sanctioned by your organization, devlop collaborations with groups striving for the same goals in network security as yours, and become and advocate for changes

[11] WHITE PAPER. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 6322". May, 1998. URL: http://www.fas.org/irp/offdocs/paper598.htm

[12] National Infrastructure Protection Center. "Outreach/Infragard" 23 Aug 2000. URL: http://www.nipc.gov/outreachinfragd.htm,

[13] TF-CSIRT, CSIRT Coordination for Europe. 18-Apr-2001. URL: http://www.terena.nl/projects/cert/

[14] The Center for Internet Security. "CIS Charter". 1 Jan 2001. URL: http://www.cisecurity.com/charter.html#10

[15] Committee on Institutional Cooperation. "Security Working Group". 23 Apr 2001. URL: http://www.cic.uiuc.edu/1%2Dit%5Fdept/comm%5Fgroups/swg/swg.html.

that will assist your organization in achieving a safe and secure network. You will then be prepared for your daily struggle to reduce the risks associated with the use of the Internet and benefit your users by providing a reliable and efficient network.