# GIAC Certified Incident Handler (GCIH) Practical Examination

Scott Alan Sumner
March 6, 2001

# Table of Contents

## *Executive Summary*

Over the period of about 18 hours during the second week of April, a series of Internet based probes and attacks were carried using a variety of tools against one the organization's firewalls. The host was taken off the internal network, and additional monitoring was placed on both the affected system and the unaffected systems. The initiating party was identified, and the appropriate authorities were contacted. The attacks were then stopped. The individual was eventually indicted and convicted.

**Details**

At 14:29 EDT on 13APR2000, a single host on the Internet apparently initiated a series of probes. The attacks apparently came from a single source, and were directed to specifically one of the firewalls. Within a minute, our Intrusion Detection System (IDS) alerted the entire Security Team via pager. The Security Manager assembled a team composed of representatives from Operations, Legal, Compliance, Infrastructure Systems, as well as the entire Security Team.

Within 15 minutes, the firewall was disconnected from the internal network and additional monitoring tools were placed on the affected firewall and the other online firewalls. This was done is such a manner to minimize tipping the instigator off. Additionally, several packet sniffers were placed on the network near the core switches. During this period, the probes evolved into more aggressive and overt actions, characterized as a series of attacks.

At this point, the team was broken into to separate efforts, with the InfoSec Manager acting as a clearinghouse. The first team (Blue) was tasked with monitoring the integrity of the existing systems, sans the affected the firewall. The second team (Red) was tasked with gathering information about the attempts, their source and assessing the risk of exposure.

The source address was looked up using the American Registry of Internet Numbers (ARIN) database, and was owned by a dental services firm. The organization's IPS was contacted as well as the dental services firm and their associated ISP. A message was sent to the Financial Sector Information Sharing and Analysis Center, CERT and the FBI.

After 18 hours of watching the intruder, the decision was made to take the affected system offline. Legal had arranged with law enforcement to have the individual detained and deprived of access to the system. As an added measure of insurance, the firewall was rebuilt for original media prior to being placed into service. The logs were archived in accordance with procedure, and provided the appropriate authorities.

## Conclusion

In retrospect, no system appears to have been compromised. However, numerous enhancements to procedures and policies can made based on the lessons learned.

## *Environment Description*

The internal network contains a trio of load-balanced/fault tolerant firewalls, which are in parallel with a pair of VPN gateway. All of the internal (also known as “red” or “private”) interfaces of the components are connected in the enterprise’s core switches. The external (“black” or “public”) interfaces are concentrated in a switch, which is patched into a router.

The firewalls normally operate in a cluster (Figure 1); however, during the event they were operating independently. The firewalls are Unix based, with a tri-homed design.

The third, or service, interface provides a region of slightly less stringent security in order to expose certain services to browsing from the Internet. There are several servers in this area, also known as the DMZ. A host based intrusion detection system resides on all three firewalls, on all three interfaces.

The firewalls are hardened, which includes an aggressive program of patch/hotfix maintenance, checksum on binaries, hashing of log files, removal of non-necessary services, shadow logging and an intense auditing program.

A honeypot sits in parallel to the firewalls and the VPN gateways. It purpose is two-fold: It provides a data gathering point for intrusion, and it acts as a “sacrificial anode” – that is, it should be easier for the intruder to compromise this rather than the hardened firewalls and VPN gateways. At the time of the incident, the honeypot was a dead-ended Microsoft Windows NT Server 4.0, patched to SP 3. This provides plenty of opportunity for someone who was looking to break into a system to do so in a way not to compromise the rest of the firm.

For logging purposes, a logging server connected to a large array of disks receiving next-day logs from the firewalls, is located on the internal network. It is also hardened, and the logs copied to tape daily. The tapes are moved off-site at the end of the month.

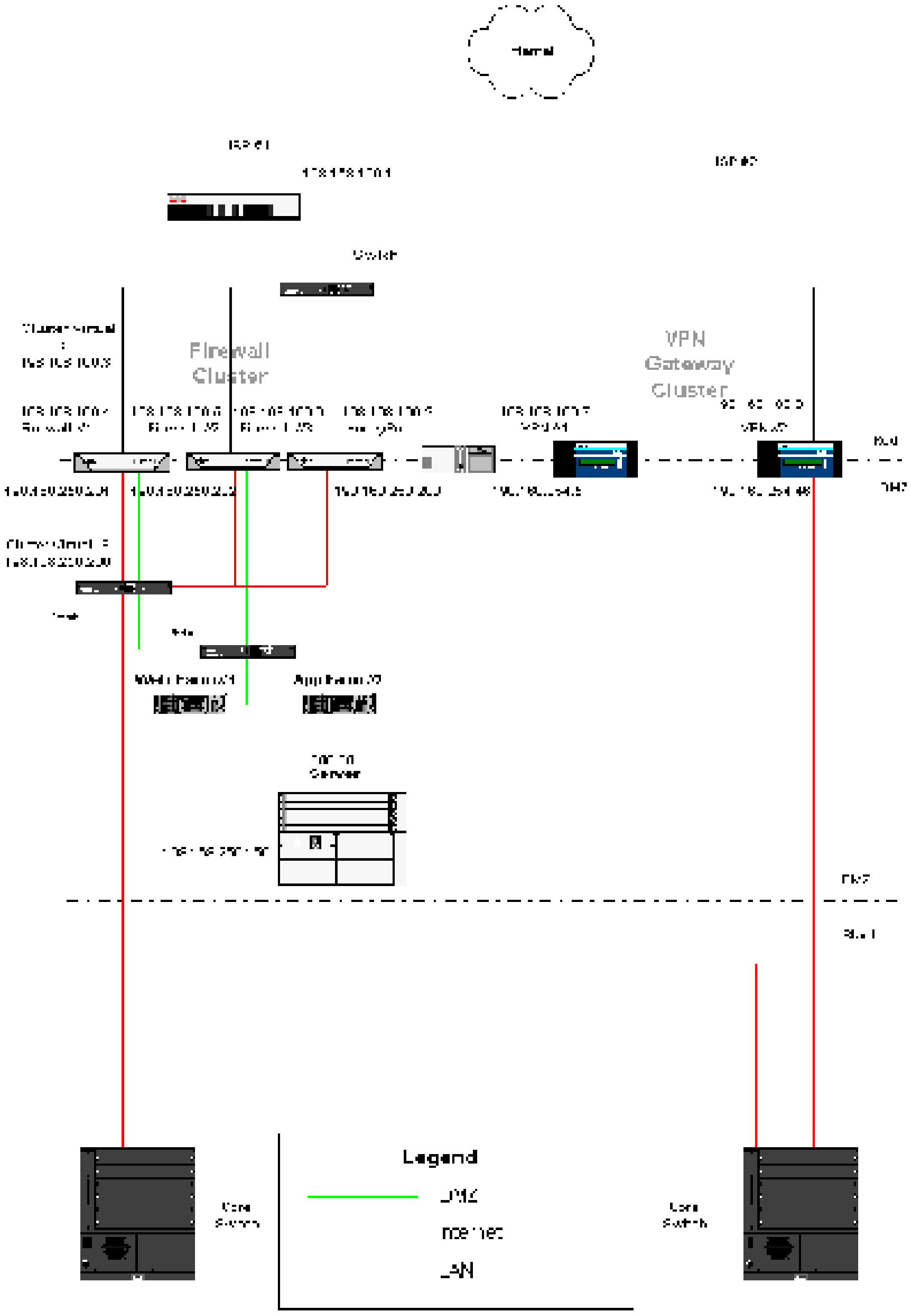


Figure 1 – Nominal Firewall Configuration

## *Incident Stages*

### Preparation

This phase is defined as the effective measures in place that would mitigate any compromise or potential harm to the organization. It is composed of a blend of policy, process, people and hardware operating in a systemic manner. In the context of this specific organization, the preparation steps include:

Policies & Procedures – A clear and concise Acceptable Use Policy (Appendix 1), communicated to every user of the organization's system. This includes full time employees, contractors, business partners, clients, interns and part-time employees. A statement attesting that the Policy has been read must be signed and filed by every individual before access is granted.

Warning Banners – A warning banner describing the penalty for inappropriate use had been placed on certain systems. It reads:

```
NOTICE: This system is the property of the <organization name
sanitized>, and is for authorized use only. Unauthorized access or use
is prohibited, and violators will be violated to the full extent of the
law. All software, data transactions, and electronic communication are
subject to monitoring.
```

Redundant Components – As much as possible, redundant components designed to failover automatically have been built into the environment. This allows for failover or swapping out of systems that have failed, or have been compromised.

HoneyPot – This component has two purposes: First, it acts as a point where the least amount of effort would be required to compromise, yet it is engineered to alarm the appropriate personal if it is accessed at all. Second, it provides another mechanism to gather information about purported attackers.

Intrusion Detection System – Six months prior to the incident, a host-based IDS was implemented. It turned out to one of the more effective measures implemented. The system maintains an inventory of signatures, which it compares against the traffic it monitors. If it makes a match, it spawns a series of automatic events, which can page a human, shutdown a service, block an IP address or range of IP addresses or merely note the event in a daily log.

Logging System – This abstracts the logging from the firewalls as much as possible, to help reduce the potential that an attacker who has gained access would change the logs to hide their tracks. Additionally, the logs are hashed to help minimize the potential for tampering. It also allows for a certain amount of combined data mining to occur on the logs due to their centralized location.

Evidence Custodianship – Several members of the Security Team had been formally trained in evidence collection, and procedural support had been implemented into the Firm's Policy and Procedures. These procedures are subject to outside auditing as well.

Disaster Recovery Plan –Although the plan was engineered more toward a general disaster such as a data center flooding or fire, a tested and refined Disaster Recovery Plan was coupled to a Business Continuity Plan in order to assure that the firm had the ability to conduct business under duress.

Good Interdepartmental Cooperation – With a single exception, all the appropriate areas of the organization were brought to bear quickly and involved intimately with the effort.

Good Calling Tree – The department office administrator was very aggressive about keep an up-to-date copy of the entire departments home, cell, pager and office phone numbers at each person's home. This was extended for certain individuals to include extra-departmental key personnel.

It is important to note that although certain enhancements could be made, a decision by Senior Management was made to accept certain risk due to the cost of the enhancements when compared to the maximum impact of the specific risk. It is the best interest of the organization not to detail those embraced risks in this document.

It was difficult to quantity the amount of work put into this step that specifically applied to this event, however, more than 1500 man-hours were involved in this step for the items mentioned above.

## Identification

This phase is defined as the steps necessary to determine whether an incident has occurred, and the nature of the incident.

IDS – The single most important contributor to the detection of this event was the host-based Intrusion Detection System. The organization SNMP system would have probably trapped on some of the events generated by the probe/attacks, but the earliest that these would have been seen was during the follow day's log review. Although, undue reliance on the IDS should be avoided, however, it is a valuable tool.

Division of Labor – One of the more important pieces of information generated by the Intrusion Detection System was the source IP address of the host initiating the attack. It is possible that the address was spoofed, but this possibility was downgraded due to the un-subtle nature of the attack. The possibility that the attack was a distraction for a more subtle attack elsewhere in the organization's infrastructure was brought up. As a result, early on in the incident, two teams were formed: One (Blue) was tasked to monitor the non-affected network, and another (Red) was tasked of containing, and tracking the intruder. It was crucial that each team communicated with one another in a manner to support its respective counterpart's efforts. The responsibility for managing both teams fell to the acting incident manager, the organization's Security Manager. Both teams were reminded of the importance of detailed note taking.

The first major task, which was shared by both teams, was to define the extent of the attack. The affected firewall was disconnected from the internal network, by unplugging the intermediate switching device that was situated between the firewall and the core switch. The presence of this switch was purely coincidental, and was due to troubleshooting of the load balancing system. The purpose of this was to avoid tipping the attacker.

**Red Team**

The decision to aggressively develop an information pool about the source IP was initiated. The first check, a "whois", checks an IP against the national registry in order to determine the owner. There should be little chance that attacker would know that this information was being accessed, unless the compromise was complete. As a measure of insurance, a stand-alone PC with dial access to a shell account externally hosted was used for supporting the investigation methods. The whois revealed that a Dental Service Company in an adjacent state owned the IP address.

Some discussion concerning the potential of the addressed being spoofed was conducted; however this was discounted because the effort wasn't specifically denial of service oriented and the attack was blatant and somewhat simpleminded. Once again, the point that this might be a distraction was considered, but in the absence of evidence of additional intrusion (particularly ones of a more sophisticated nature) was revealed, the plan was to continue to prosecute the target of interest.

There were approximately 10 man-hours put into this stage relative to this event.

## Containment

This phase describes the steps necessary to limit the scope and magnitude of an incident, to keep the incident from getting worse.

**Blue Team**

Define limits of compromise – The IDS's on the other firewalls were tested, the logs of each firewall and the honeypot inspected for symptoms of compromise. Comparisons of the firewall under attack and the other firewall logs were made. Dialup Service Call Detailing Logs were examined as well as other logs on various strategically located servers. Additionally, various other points of entries were examined, such as PBX call detail logs, RAS servers, VPN servers and such.

After an initial assessment, the decision was made to place packet sniffers in strategic points in the network. "Spanning" the port on the switch going into the affected firewall to another port (which the sniffer was then plugged into), minimized the potential for detection of the promiscuous mode sniffers, albeit remote.

Collection of Evidence – The decision of backing up the firewall was deferred until the normal backup period, to avoid tip-off. New media was used, and was treated as evidence from the point the blank tape was taken off the shelf.

The backup was made, bagged and tagged. Use of the two-man rule was maintained.

There were approximately 15 man-hours put into this stage relative to this event.

## Eradication

This phase is defined as the steps necessary to eliminate the threat and prevent future compromise using the same or similar methods.

Disconnect affected systems – The planned method of removing the threat was straightforward. After a period of 18 hours after the initial detection, the affected system was turned off. This was done in conjunction with the detaining of the alleged attacker. The effectiveness was reinforced (although not entirely confirmed) by the cessation of the probes.

Particular care was taken in this approach since the damage created if the wrong individual was detained, not only would the attacks be stopped, but incalculable damage would be done to the organization. It would be exponentially more difficult to get a second person stopped.

Prevent Future Compromise – Until a complete analysis of the tools used, the ability to determine the attacking tool set was limited to what was actually seen by the firewall. Since it was determined that there was no penetration at the end of the incident, there was no specific task to implement changes necessary to protect from the compromise. However, there was a need to examine other potential holes, and that was a to-do item discussed during the follow-up phase.

There were approximately 45 man-hours put into this stage relative to this event.

## Recovery

This phase is the steps necessary to restore the affected systems to operation readiness, while maintaining the integrity of the evidence.

Rebuild and Restore – In this instance, the firewall was rebuilt from scratch. Two days after the cessation of the attacks, it was restored to service. The actual restoration is detailed in the Backup/Restoration Section.

Evidence – The evidence was kept in a secured location until it was remanded to the custody of law enforcement. A signature was requested and obtained from the law enforcement official who collected the evidence.

There were approximately 115 man-hours put into this stage relative to this event.

## Follow-up

This phase is defined as the process, which deficiencies are identified, and an analysis is made in order to implement the changes necessary to improve the organizations efforts to respond to incidents such as this.

The debriefing session was started as soon as it was feasible to do so, and the entire group participated in the production of the proposal. The proposal was submitted to management, and project teams were assigned to various projects.

After the group had an opportunity to get some sleep, an extended debrief was held, during which deficiencies were discovered and recommendations made:

**Planning Phase**

The most significant item identified was lack of using outside resources for intrusion detection, risk mitigation or incident handling. Organizations such as SANS and FS/ISAC (as well as many others) provide information and other perspectives. The only investment is time – operating in a vacuum leads to blind spots.

Senior management tended to rely on hardware only as a cost mitigation technique – It was fortunate that senior management identified this as a shortcoming; as it would be difficult to implement with their support.

No standardized checklists existed prior to the incident. As a result, several tasks that should have been done were not performed. For example, participation in the incident by the Public Affairs Office was omitted.

Warning Banners should be placed on all systems, not just the firewalls.

Training of the team was strictly done ah hoc basis, and not necessarily complementary to the skills or roles of the team members. Target analysis process requires some formal training. This was one of the weakest components, simple due to the lack of education and training. The proposed refinements included aggressive training plans for several team members in every area.

No compensation plan was in effect. Compensation is more than simply a salary adjustment; examples of non-standard compensation include: Additional vacation, telecommuting, flextime, trips, larger work area and items such as flat-screen monitors. The manager of the each employee determines the nature and timing of the compensation. However, senior management takes an interest in this specific item, so that it is applied fairly and uniformly without making it generic.

Although the Disaster Recovery Plan has a notification tree in hard copy, there was no treatment of an out-of-band communication plan. If the system had been compromised, corporate email would not be an appropriate mechanism of communication.

Although the complete list of passwords is kept in a safe, which can be accessed by any IT supervisor, a system for maintain of cryptographic keys for secure communication should also exist.

Unexpectedly, most of the team was extremely aggressive about time keeping, which was not quite as difficult as it might, as all the hosts involved were in the same time zone.

There was a good deal of effort to maintain the physical comfort level of the participants. This was not as altruistic as it might seem – tired and hungry people are more likely to make mistakes. Hotel Rooms and pizza as well as coffee flowed freely.

Some discussion was made concerning additional systems, such as packet filter on the router level as well as a node-based IDS used to supplement the current systems. The list of recommended modifications were itemized and submitted as part of the proposal. The management's response was a mandate to further research this and provide a subsequent proposal after the other refinements had been made.

A examination of potential design considerations built directly into the network fabric (for example, Router ACL's, router/switch password rotation, etc.) was recommended.

A detailed examination of the forensic and information gathering tool kits was recommended.

Prior to the incident, there were no formal or informal relationships with any law enforcement body. Subsequent application to several organizations, including the local InfraGard chapter, was made. Contacts were made, and periodic meetings with representatives of the State Police, the City Police, and the City management are being held.

There is no easy reporting facility. A single clearing house of incident reports was created in the Operations area.

**Identification**

The Security Manager was tasked as the incident manager, and the single point of contact. This person was also the Intrusion Detection analyst; it would probably be best if those duties were separated.

It continues to be a very subjective and difficult task to determine whether an event is an incident. The best mechanism seems to be repeated reviews by several individuals who should be seasoned network engineers, and ideally, intrusion analysts. Formal training was mandated.

At the point where a positive determination that an incident has occurred, a structured reporting mechanism needed to be engineered. This needs to include organization management by law enforcement as well.

It was believed that a provable chain of custody of all potential evidence was maintained in accordance with standard industry practices. However, continuous reviews of these practices need to be made on an ongoing basis.

**Containment**

Using traceroute to the alleged intruder's IP address could have tipped him/her off. Other non-intrusive methods should have been used.

There was some uncertainty of the wisdom of leaving the targeted system online. The concern was that even separated from other targets of opportunity, simply having root level access (which was never achieved) would provide a wealth of implementation information that could be used for future attacks. The consensus was that the decision was correct in the context of this incident, and future incidents would have to be judged on a case-by-case basis.

It was unfortunate that the honeypot was not the target. It would have been a learning opportunity as well as abstracted completely from the production network.

Although the Disaster Recovery Plan was a good baseline, the entire process would benefit from documenting standard procedures. These procedures would more than likely evolve over time, but they help ensure nothing is forgotten.

Although the attack was not serious enough to consider closing up shop, and transferring production services to an alternate location, this might not always needs to be the case. At a minimum, the alternate location should be placed on alert as soon as the potential for such a situation exists.

The team structure seemed to work well. Communication between the teams was scheduled, in order to provide each group the supporting information that it needed to perform its tasks effectively.

The information about the incident was not controlled as well as it should have been. A balance has to be struck between availability of the information and limiting the information to those who have a need to know. The incident manager should be responsible for this. Additionally, a central and secure "Command Center" should have been established for the duration of the incident. This center should have phone, faxes lines and outside lines (analog POTS lines vice PBX extensions). Periodic and scheduled reports should be mandated. Finally, the center should have access to all pertinent policies and procedures as well as the calling lists.

The system was left intact until a complete forensic backup was made. Additionally, two routine backups were made to new media and retained as evidence. For the analysis itself, a working copy, and not the originally backed up tapes were used, in order to preserve the sanctity of the copies. Again, procedures for control of evidence were maintained.

The firewall was pretty much left alone after the intrusion. This was primarily due to potential that the firewall might have been compromised. Of course, once it was disconnected from all networks, then it could be examined. Before the examination was begun, the firewall was backed up to new media. It was unfortunate that the firewall did not allow for hot removal of one of a set of mirrored drives.

**Eradication**

The cause of the probes/attacks was determined, although in a flawed fashion. The mechanism was eventually determined through analysis of the initiating host was a suite of tools made available to the intruder. Law enforcement is pursuing the original source of the tools.

A good deal of effort was expended to ensure that the system was not compromised. The firewall and associated infrastructure make liberal use of checksums and hashes, for both binary verification and as an anti-tampering mechanism for the logs. An examination of processes running and other tell-tales of Root Kit Implementation were also exhaustively examined.

An IDS is only as good as it's signatures. A continuous effort to refine the signature database to improve defenses is crucial.

A top down vulnerability analyses for IT systems, component based and network as well as process review was deemed to be prudent.

**Recovery**

The goal with this was to restore the system without restoring any potential compromise. The best way to do that was rebuild the system from scratch. This was done, and the system was subjected to the same rigorous review as was performed during the eradication phase.

In order to validate the system, the firewall was submitted to the same acceptance criteria as any new system placed online. Some members of the team felt that this was overkill, but the overriding theme of conservatism prevailed. It didn't take much longer, and provided a larger feeling of comfort.

Patch application at the firm was driven by business need – that is, if something didn't work, then the patch was applied. This is flawed, so an ongoing patch review and installation board was created in order to ensure that patches were aggressively tracked, reviewed, tested, validated and installed in a timely manner.

The decision on when to restore the firewall to service was determined by the availability of the restored box. Since system performance was not significantly degraded by the lack of the firewall, undue pressure did not exist to prematurely install the firewall. This factor may not exist in other situations, and there must be a balanced decision making process at any time such a system is restored. The mistake made concerning the firewall is the box itself should have been removed as evidence, as a complete unit.

Although heightened awareness continued for a while, the passage of time diminishes the quality of the scrutiny on the entire enterprise. Therefore, it is paramount that a systematic audit and review of logs, alerts and reviews be maintained indefinitely.

**Additional Tasks during the follow up phase**

A Report to CERT was made as soon as the intrusion data was confirmed. A follow-up report was not sent for several weeks, however.

In order to maximize data collection, all logs for systems on the boundary of the Internet, as well as temporary systems like the packet sniffer were packaged in the evidence deliverable. In retrospect, there might be value in providing some additional logs of systems immediately adjacent to these systems (SNMP Management logs, DMZ Web Server logs, etc.) as well.

It would be interesting to be able to obtain the exact suite of tools used and replicate the attack in a lab environment. Until the case is brought to court, that may not be possible.

It is difficult to quantify the number of hours put into this phase if implementation times are included for new processes and systems. However, for the review itself, there were approximately 180 man-hours put into this stage relative to this event.

## *Detailed Chronology*

# *DAY 1*

**EVENT:** IDS Alert #1
**TIME:** APR13 14:29:32 EDT
**DETAIL:**

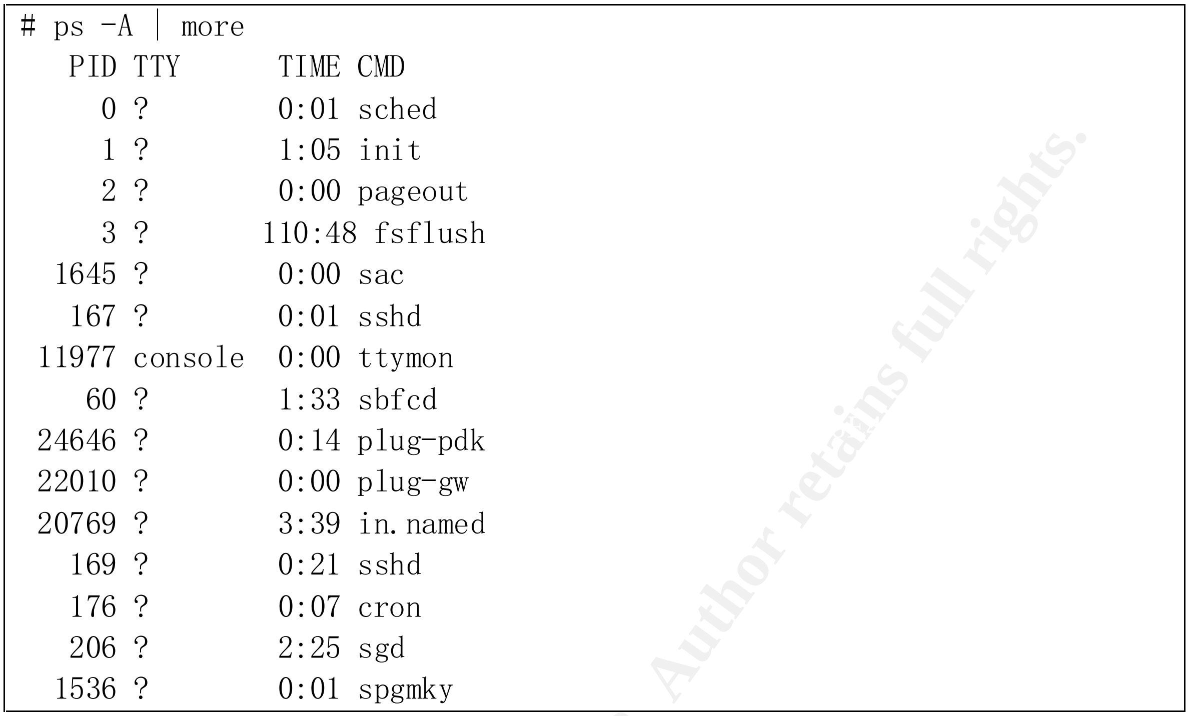
```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: unknown Date: Thu Apr 13 14:29:32 2000 Reason: Denied Remote
Login
Summary: attacked gwy.targethost.com 192.168.100.66 unknown Denied
Remote Login BLOCKED
Cause: Apr 13 14:29:17 attackedgwy.targethost.com tn-gw[21549]: deny
host=unknown/192.168.100.66 use of proxy
Status: blocked from network until Thu Apr 13 15:29:17 2000
```

**EXPLANATION:**
Fairly common, the organization sees 2-3 a month. The IDS Alert trigger is set for 2 failures. The Security Group usually takes a cursory look at the systems – see next entry.

---

**EVENT:** Security Team responded to page
**TIME:** APR13 Circa 14:35 EDT
**DETAIL:**

After logging into the firewall directly using the console, the first thing the Team tries to do is to run "ps –A | more" to look for extraneous processes (Figure 2).



```
# ps -A | more
   PID TTY      TIME CMD
     0 ?        0:01 sched
     1 ?        1:05 init
     2 ?        0:00 pageout
     3 ?       110:48 fsflush
  1645 ?        0:00 sac
   167 ?        0:01 sshd
 11977 console  0:00 ttymon
    60 ?        1:33 sbfcd
 24646 ?        0:14 plug-pdk
 22010 ?        0:00 plug-gw
 20769 ?        3:39 in.named
   169 ?        0:21 sshd
   176 ?        0:07 cron
   206 ?        2:25 sgd
  1536 ?        0:01 spgmky
```

Figure 2 – Example of baseline “ps –A” of firewall

The team would also run a “top” to look at utilization/health (figure 3).

```
last pid: 23313;load averages:0.04,0.16,0.18                        20:35:08
186 processes: 185 sleeping, 1 on cpu
CPU states: 91.4% idle,0.4% user,5.7% kernel,  2.5% iowait,  0.0% swap
Memory: 1024M real, 16M free, 600K swap in use, 1915M swap free

  PID USERNAME THR PRI NICE  SIZE   RES STATE   TIME    CPU COMMAND
11520 root       1  58    0   29M   29M sleep  19.3H  1.57% fwdm
23313 root       1  20    0 2096K 1592K cpu     0:00  1.43% top
20003 root      13  25    0 3128K 1784K sleep   8:00  0.86% syslogd
23228 root       1  58    0 2416K 1992K sleep   0:01  0.08% sshd
20323 root       1  59    0 2040K 1304K sleep   0:00  0.05% spgmky
20769 root       1  58    0 5784K 5312K sleep   3:38  0.03% in.named
 1600 root      12  59    0 3648K 2008K sleep   0:20  0.02% spgmky
   60 root       6  59    0 3856K 1952K sleep   1:33  0.02% sbfcd
 1474 root       1  48    0 2112K 1136K sleep  10:16  0.01% snmp-mod
23305 root       1  43    0  872K  736K sleep   0:00  0.01% sleep
 1602 root      12  59    0 4272K 2848K sleep   0:31  0.01% spgmky
11521 nobody     1  58    0  832K  600K sleep  10:24  0.00% unlinkd
 1579 root      17  58    0 4160K 2792K sleep   7:39  0.00% spgmky
  206 root       1  33    0  960K  784K sleep   2:25  0.00% sgd
 1589 root      12  59    0 3816K 2408K sleep   2:17  0.00% spgmky
```

Figure 3 – Example of baseline "top" of firewall

Finally, a quick tail of the logs, looking for anything unusual, but failed authentications specifically.

```
# tail access.log
983583399.623    191 198.168.252.252 TCP_MISS/200 1359 GET
http://www.briefing.com/sub/stocks/Clock.htm - DIRECT/www.briefing.com
text/html
983583417.174    168 198.168.252.252 TCP_MISS/200 1359 GET
http://www.briefing.com/sub/stocks/Clock.htm - DIRECT/www.briefing.com
text/html
```

Figure 4
Example of baseline "tail access.log"

**EXPLANATION:** Everything at this point looked nominal. The event was noted in a log used for trend analysis.

**EVENT:** IDS Alert #2
**TIME:** APR13 14:43:57 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:43:57 2000
Reason: echo/chargen packet flood
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
echo/chargen packet flood BLOCKED
Cause: Apr 13 14:43:56 attacked gwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1643 dstaddr=198.168.100.4 dstport=19
Status: blocked from network until Thu Apr 13 15:43:56 2000
```

**EXPLANATION:**
(CVE-1999-0103) This has gone from a very innocuous probe to an apparently direct attack. The IDS responds by dropping traffic from that IP/port combination for a pre-determined period of time automatically. It also pages the Security Team again.

---

**EVENT:** IDS Alert #3
**TIME:** APR13 14:44:01 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:44:01 2000
Reason: Well Known Port Scanning
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 Well
Known Port Scanning BLOCKED
Cause: Apr 13 14:43:56 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1624 dstaddr=198.168.100.4 dstport=1
Status: blocked from network until Thu Apr 13 15:43:56 2000
```

**EXPLANATION:**
This happens extremely quickly after the last one (<4 seconds). That coupled, with the aggressive flood followed by the scan (vice the reverse) implies an automated tool, or suite of tools. The firewall management group has taken notice of the events at this point.

**EVENT:** IDS Alert #4
**TIME:** APR13 14:44:18 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:44:18 2000
Reason: RPC probe
Summary: attacked gwy.targethost.com 192.168.100.66 198.168.100.4 RPC
probe BLOCKED
Cause: Apr 13 14:44:17 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=2677 dstaddr=198.168.100.4 dstport=111
Status: blocked from network until Thu Apr 13 14:45:18 2000
```

**EXPLANATION:**
Another probe, launched very quickly after the previous one. RPC vulnerabilities are prevalent and dangerous if exploited.

---

**EVENT:** IDS Alert #5
**TIME:** APR13 14:45:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:45:00 2000
Reason: CheckPoint Firewall-1 Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
CheckPoint Firewall-1 Probe BLOCKED
Cause: Apr 13 14:44:59 attacked gwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=4750 dstaddr=198.168.100.4 dstport=256
Status: blocked from network until Thu Apr 13 14:45:59 2000
```

**EXPLANATION:**
(CVE-1999-0675) More support for the theory this is at least partially automated or scripted. This was an attempt to use a firewall specific probe.

---

**EVENT:** Discussion
**TIME:** APR13 Circa 14:45:00 – 15:00:00 EDT
**DETAIL:**
Legal, Operations, Compliance and Senior Management are notified by out-of-band means. The firewall team confirms that the logs on the other two firewalls do not reflect the same sort of activity occurring. The decision is made to disconnect the internal interface of the firewall. The consensus was that this should be done with the following provisions:

1) Other points of entries should have increased surveillance placed upon them. If any activity is detected, the affected system will be pulled from service as soon as practical.

2) Every effort should be made not to tip off the intruder. By pure coincidence, the internal interface of the affected firewall had a small switch between it and the rest of the network, so a message detailing the disconnection of the cable from the interface would not be generated.
3) The firewall was to be treat as a crime scene. The number of folks accessing it were limited to the number of people who could crowd around the console.

The team planned to meet every hour, until a major event occurred.

**EXPLANATION:**

First priority was to preserve the ability of the organization to function, but the secondary goal was to prosecute this individual. Keeping a low profile would help this.

---

**EVENT:** IDS Alert #6 EDT

**TIME:** APR13 14:53:04

**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:53:04 2000
Reason: IBM Firewall Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 IBM
Firewall Probe BLOCKED
Cause: Apr 13 14:53:03 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1203 dstaddr=198.168.100.4 dstport=2001
Status: blocked from network until Thu Apr 13 14:54:03 2000
```

**EXPLANATION:**

(CVE-2000-1038), et al. This seems to be more of the same style of probe. Each probe/attack is different, as if a script of scripts is running. Another firewall specific probe. This attacker is hunting in a very unsubtle, hit or miss fashion.

---

**EVENT:** IDS Alert #7

**TIME:** APR13 14:57:38 EDT

**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 14:57:38 2000
Reason: ISS RealSecure Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 ISS
RealSecure Probe BLOCKED
Cause: Apr 13 14:57:37 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=3205 dstaddr=198.168.100.4 dstport=2998
Status: blocked from network until Thu Apr 13 14:58:37 2000
```

**EXPLANATION:**

(CAN-2000-0692), et al. Another, and different, probe.

**EVENT:** Internal Interface Removed from Internal network
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**
The CAT-5 cable from the small switch to the core switch was moved to the Ethernet port on a throwaway laptop.
**EXPLANATION:**
Primarily, this was to segregated a host that was on it's was to being compromised from the rest of the organization's assets. It also provided an additional vantage point in order to provide as much data as possible. Additionally, it allowed for pre-positioning of certain tools (for example, dd, for use during the recovery phase).

---

**EVENT:** Discussion
**TIME:** APR13 Circa 15:05:00 EDT
**DETAIL:**
The Security Manager decided to provide some additional structure around the responses. To this end, two teams were created. The "Blue" Team was to preserve the integrity of the existing production systems by intense monitoring. The "Red" Team was to contain and track the intruder. Representation from most areas was evenly divided, at least as much as possible. Emphasis was made on documenting as much as possible
**EXPLANATION:**
It is conceivable that this activity might be a cover for more subtle attacks from another perspective.

---

**EVENT:** IDS Alert #8
**TIME:** APR13 15:11:20 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:11:20 2000
Reason: X probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 X
probe BLOCKED
Cause: Apr 13 15:11:17 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1252 dstaddr=198.168.100.4 dstport=6000
Status: blocked from network until Thu Apr 13 16:11:20 2000
```

**EXPLANATION:**
(CAN-1999-0623) et al, A common X-windows probe , and the Trojan ("the Thing") uses this port as well.

---

**EVENT:** RED TEAM – Whois lookup
**TIME:** APR13 Circa 15:15 EDT
**DETAIL:**
On a privately owned, dialup shellaccount (e.g., coming from another IP Class B), the whois was run:

```
spacebaby: # whois -h rs.arin.net 192.168.100.66
The numbskil Group Co. (NETBLK-NUMBSKUL-1)
   123 Bonehead Ave
   Crackhead, NY 00000
   US

   Netname: NUMBSKUL-1
   Netblock: 192.168.100.0 - 192.168.199.254

   Coordinator:
      Bright, Iam Notso  (XXT-ORG-ARIN)  hostmaster@numbskul.com
      212-555-1212 ex-666
       Fax- 212-555-2323

   Domain System inverse mapping provided by:

   DNS1.NUMBSKUL.COM            192.168.1.1
```

**EXPLANATION:**
An attempt was made to be objective as possible, because address spoofing and other subterfuge is possible. A notebook was kept, with hard copy of all the output generated by this research.

**EVENT:** RED TEAM – Tracert
**TIME:** APR13 Circa 15:16 EDT
**DETAIL:**
On a privately owned, dialup shell account (e.g., coming from another IP Class B), a trace of the IP was run:

```
Spacebaby: traceroute 192.168.100.66

 1   traceroute to 192.168.100.66 (192.168.100.66), 30 hops max, 40 byte packets
 2   gw.customer.com (198.168.100.1)  3 ms  4 ms  2 ms
 3   s1-1-0-15-0.nyc.anyisp1.net (198.168.40.40)  7 ms  3 ms  3 ms
 4   rtr2-anyisp1.net(198.168.50.50)  15 ms  15 ms  14 ms
 5   entre-anyisp1.net (198.168.99.99)  44 ms  19 ms  29 ms
 6   backabone-anyisp2.net (192.168.99.99)  18 ms  25 ms  17 ms
 7   intrtr2-anyisp2.net (192.168.30.30)  21 ms  26 ms  20 ms
 8   intrtr2-anyisp2.net (192.168.20.20)  22 ms 27ms 22 ms
 9   custgw-anyisp2.net(192.168.10.10)  53 ms  24 ms  28 ms
 10  192.168.100.10 (192.168.100.10) 45 ms 22 ms 24 ms
 11  192.168.100.66 (192.168.100.66) 68 ms 24 ms
```

**EXPLANATION:**
It looks like that if this is the real host of the originating attacks, it is probably someone uses another organization host to launch the attack. What's more, there's a reasonable good chance the hop #9 is a managed firewall – although not managed real well, if it's letting stuff like this through.

---

**EVENT:** IDS Alert #9
**TIME:** APR13 Circa 15:14:28 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:14:28 2000
Reason: irc chat DOS
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 irc
chat DOS BLOCKED
Cause: Apr 13 15:14:26 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=2614 dstaddr=198.168.100.4 dstport=6667
Status: blocked from network until Thu Apr 13 16:14:28 2000
```

**EXPLANATION:**
(CVE-2000-0594) A Denial of Service attack, probably although some well known trojans look for port 6667 (ScheduleAgent, Trinity, WinSatan). Later analysis developed the theory that it might have been one of the "bitch" genre IRCDOS attacks, but modified. This is overtly hostile.

---

**EVENT:** IDS Alert #10
**TIME:** APR13 Circa 15:24:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:24:00 2000
Reason: Gauntlet Remote Admin
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
Gauntlet Remote Admin BLOCKED
Cause: Apr 13 15:20:44 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1352 dstaddr=198.168.100.4 dstport=8001
Status: blocked from network until Thu Apr 13 16:24:00 2000
```

**EXPLANATION:**
(CVE-1999-0683) Another firewall specific attack.

---

**EVENT:** IDS Alert #11
**TIME:** APR13 Circa 15:32:44 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:32:44 2000
Reason: Gauntlet Remote Admin
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
Gauntlet Remote Admin BLOCKED
Cause: Apr 13 15:26:56 [198.168.100.4] unix: securityalert: packet
denied by local screen: TCP if=hme0 srcaddr=192.168.100.66 srcport=4030
dstaddr=198.168.100.4 dstport=8001
Status: blocked from network until Thu Apr 13 16:32:43 2000
```

**EXPLANATION:**
(CVE-1999-0683) This is the first duplicated style probe. Why?

**EVENT:** IDS Alert #12
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:37:38 2000
Reason: CheckPoint Firewall-1 Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
CheckPoint Firewall-1 Probe BLOCKED
Cause: Apr 13 15:37:35 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1838 dstaddr=198.168.100.4 dstport=18183
Status: blocked from network until Thu Apr 13 15:38:38 2000
```

**EXPLANATION:**
(CVE-1999-0675) Another Duplicate.

---

**EVENT:** IDS Alert #13
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Thu Apr 13 15:37:29 2000
Reason: TFN2K/Stacheldraht DOS
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
TFN2K/Stacheldraht DOS BLOCKED
Cause: Apr 13 15:37:11 [198.168.100.4] unix: securityalert: packet
denied by local screen: TCP if=hme0 srcaddr=192.168.100.66 srcport=1666
dstaddr=198.168.100.4 dstport=16660
Status: blocked from network until Thu Apr 13 16:37:28 2000
```

**EXPLANATION:**
(CAN-2000-0138) This was something new to us. We had heard of The Tribal Flood Network, but no-one had researched it to the point of understanding “Stacheldraht”, or “Barbed-Wire”, Distributed Denial of Service Attack. Initially, it was unclear whether this was, after some investigation it was discovered on the CERT website.

---

**EVENT:** IDS Alert #14
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceName: imaginary.enemy.net
SourceAddr: 191.168.2.2
DestAddr: unknown
Date: Thu Apr 13 22:55:34 2000
Reason: Denied Remote Login
Summary: attackedgwy.targethost.com 191.168.2.2 unknown Denied Remote
Login BLOCKED
Cause: Apr 13 22:55:29 attackedgwy.targethost.com tn-gw[13268]: deny
host=unknown/191.168.2.2use of proxy
Status: blocked from network until Thu Apr 13 23:55:29 2000
```

**EXPLANATION:**

This was probably unrelated, and given the proximity of the source address to the real address of the outside interface, it might even be accidental.

---

**EVENT:** IDS Alert #15
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 03:47:37 2000
Reason: X probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 X
probe BLOCKED
Cause: Apr 14 03:47:36 [198.168.100.4] unix: securityalert: packet
denied by local screen: TCP if=hme0 srcaddr=192.168.100.66 srcport=1252
dstaddr=198.168.100.4 dstport=6000
Status: blocked from network until Fri Apr 14 04:47:36 2000
```

**EXPLANATION:**

A common X-windows probe, and the Trojan ("the Thing") uses this port as well.

---

**EVENT:** Attacker ISP Contact
**TIME:** APR13 Circa 16:00:00 EDT
**DETAIL:**

The attacker's ISP was contacted by phone and in writing. They seems to be very responsive, but were also respective of their customer's privacy.

**EVENT:** Organization ISP Contact
**TIME:** APR13 Circa 16:15:00 EDT
**DETAIL:**

The organization's ISP was contacted by phone and followed up in writing. Contrary to the experience by the ISP of the attacker, they were reluctant to provide any information, or even to show interest.

---

**EVENT:** Local Authority Contact
**TIME:** APR13 Circa 16:30:00 EDT
**DETAIL:**

The local police were contacted; unfortunately they did not have the trained resources available to assist directly. However, they were kept informed of the events as they continued to occur. This was done partially as a courtesy, but also to encourage them to obtain such expertise in the future.

---

**EVENT:** Federal Authority Contact
**TIME:** APR13 Circa 17:00:00 EDT
**DETAIL:**

The federal law enforcement agency responsible for this sort of white-collar crime was contacted, and was extremely responsive. It was immediately apparent that the bulk of evidence collection responsibility would fall upon the organization.

---

**EVENT:** Contact with the firm that apparently owns the host that this is launched from (hereafter referred to as "the firm)
**TIME:** APR13 Circa 15:03:00 EDT
**DETAIL:**

The firm was contacted, and in an effort to limit risk, was asked to look into the incident. There was some confusion on their end, because the name of the individual was provided (without asking), and then they denied ever having a person with this name working at the firm. The firm then disconnected.
On a subsequent call, the attorney's for the hosting firm stated that the user job was to do that the firm, as his father was the head of security of the target organization, and had asked for the "Security Profiling". This was particularly bizarre since:

1) The firm was in the business of providing dental services.
2) The Security Manager for the Organization was also on the call. He had not granted any permission for any individual to conduct any assessment.
3) The Security Manager also stated that his sole offspring was too short to reach the keyboard, as he was only two years old.

At that point, the attorney for the firm promised to look into as soon as possible.

---

**EVENT:** Meeting
**TIME:** APR13 Circa 17:00:00 EDT
**DETAIL:**

Both Teams met and discuss the day's events. Legal had initiated contact with the firm that allegedly owned the host, and had asked them to "look into it". Whether or not they complied was the subject of vigorous discussion, but any further decisions (barring any significant changes) were deferred for a period of 24 hours.
The next topic of discussion was subject of the evening and graveyard shifts. Since no attacks occurred after 3:00 in the afternoon, the possibility that this was someone on the job occurred. However, some individuals had to continue monitoring in order to maintain integrity. Volunteers were sought and assigned specific monitoring tasks. Hotel rooms adjacent to the organization were obtained, as well as food and other amenities.

# *DAY 2*

**EVENT:** Morning Meeting
**TIME:** APR14 Circa 07:00:00 EDT
**DETAIL:**
The night crew was relieved, but before they went home and got some sleep, both Teams got together, and the proposal to sever access was made. Senior Management concurred.
**EXPLANATION:**
Legal had relayed the information that the firm allegedly hosting the activity had agreed to at least remove the individual from his environment long enough to confirm or deny that he/she was responsible. It was deemed that enough information was cached properly, and the efforts were reaching a point of diminishing returns.
The decision to sever access as soon as we could confirm that the attacks stopped, backup the DASD on the firewall and rebuild it from scratch was made. The tentative cutout time was 12:00 noon EDT, assuming that the attacker was stopped at or before 10:00 EDT

---

**EVENT:** IDS Alert #16
**TIME:** APR14 09:33:59 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:33:59 2000
Reason: echo/chargen packet flood
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
echo/chargen packet flood BLOCKED
Cause: Apr 13 14:43:56 attacked gwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1643 dstaddr=198.168.100.4 dstport=19
Status: blocked from network until Thu Apr 13 15:43:56 2000
```

**EXPLANATION:**
(CVE-1999-0103) This combination of UDP services can be used to bomb or flood a target. This is the same attack after the initial probe yesterday. Will it repeat?

---

**EVENT:** IDS Alert #17
**TIME:** APR14 09:33:58 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:33:58 2000
Reason: Well Known Port Scanning
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 Well
Known Port Scanning BLOCKED
Cause: Apr 14 09:33:57 attackedgwy.targethost.com unix: securityalert:
tcp if=hme0 from 192.168.100.66:4809 to 198.168.100.4 on unserved port
6
```

```
Status: blocked from network until Fri Apr 14 10:33:57 2000
```

**EXPLANATION:**

This is similar to Day One events.

---

**EVENT:** IDS Alert #18

**TIME:** APR14 09:34:17 EDT

**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:34:17 2000
Reason: RPC probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 RPC
probe BLOCKED
Cause: Apr 14 09:34:16 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=4914 dstaddr=198.168.100.4 dstport=111
Status: blocked from network until Fri Apr 14 09:35:16 2000
```

**EXPLANATION:**

This pretty much leads to the conclusion that was the same suite as the 13th.

---

**EVENT:** IDS Alert #19

**TIME:** APR14 09:35:00 EDT

**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:35:00 2000
Reason: CheckPoint Firewall-1 Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4
CheckPoint Firewall-1 Probe BLOCKED
Cause: Apr 14 09:34:58 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=1085 dstaddr=198.168.100.4 dstport=256
Status: blocked from network until Fri Apr 14 09:35:58 2000
```

**EXPLANATION:**

(CVE-1999-0675)

---

**EVENT:** IDS Alert #20

**TIME:** APR14 09:43:03 EDT

**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:43:03 2000
Reason: IBM Firewall Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 IBM
Firewall Probe BLOCKED
```

```
Cause: Apr 14 09:43:02 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=2843 dstaddr=198.168.100.4 dstport=2001
Status: blocked from network until Fri Apr 14 09:44:02 2000
```

**EXPLANATION:**
(CVE-2000-1038) Supports the previous argument.

---

**EVENT:** IDS Alert #21
**TIME:** APR14 09:34:17 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceAddr: 192.168.100.66     192.168.100.66
DestAddr: 198.168.100.4
Date: Fri Apr 14 09:47:42 2000
Reason: ISS RealSecure Probe
Summary: attackedgwy.targethost.com 192.168.100.66 198.168.100.4 ISS
RealSecure Probe BLOCKED
Cause: Apr 14 09:47:35 attackedgwy.targethost.com unix: securityalert:
packet denied by local screen: TCP if=hme0 srcaddr=192.168.100.66
srcport=3846 dstaddr=198.168.100.4 dstport=2998
Status: blocked from network until Fri Apr 14 09:48:36 2000
```

**EXPLANATION:**
(CAN-2000-0692) This was the last confirmed attack or probe launched by this host. If the pattern kept up, an X Probe would have occurred within the next few minutes.

---

**EVENT:** Alleged Attacker removed from his location.
**TIME:** APR14 Circa 09:40:00 EDT
**DETAIL:**
The Security Manager received a call from the firm that owned the computer that allegedly initiated these events. The user was detained, but not arrested at that point.
**EXPLANATION:**
This is the point where the organization becomes more passive and supportive in the prosecution of the individual, assuming that the attacks have been stopped.

**EVENT:** IDS Alert #22
**TIME:** APR14 09:34:17 EDT
**DETAIL:**

```
Hostname: attackedgwy.targethost.com
SourceName: kidsfun.co.uk
SourceAddr: 195.11.18.86
DestAddr: 198.168.100.4
Date: Fri Apr 14 11:15:28 2000
Reason: Well Known Port Scanning
Summary: attackedgwy.targethost.com195.11.18.86 198.168.100.4 Well
Known Port Scanning BLOCKED
Cause: Apr 14 15:15:22 [198.168.100.4] unix: securityalert: packet
denied by local screen: TCP if=hme0 srcaddr=195.11.18.86 srcport=1183
dstaddr=198.168.100.4 dstport=80
Status: blocked from network until Fri Apr 14 16:15:22 2000
```

**EXPLANATION:**

This was unexpected, however, was confirmed to be an unrelated scan. The thought that this was a "distracter" was initially tempered by the thought that this was a parallel attack. The scan was not repeated.

---

**EVENT:** Firewall Shutdown
**TIME:** APR14 12:10:00 EDT
**DETAIL:**

The external network interface of the affected firewall was unplugged. The machine was then backup, and then the hard drive was wiped.

---

Over the next few days, the following events occurred:

1) Heightened awareness gradually diminished.
2) A debrief was held after everyone was rested.
3) The firewall image was restored to a similar machine, and was forensically examined to ensure that no binaries had been compromised, or the attacker had left any other debris.
4) The image of the hard drive, the logs and several statements by employees of the organization were turned over to law enforcement.
5) A project plan was formulated to turn the Lessons Learned into projects.
6) The firewall was rebuilt from scratch, with the exception of several configuration files and system servicing scripts, which were verified to be clean after being copied from CD.

## *Firewall Backup/Restoration*

### Backup

The script “backup.sh” is run at 2:00 am (right after log rotation).

```
#!/bin/sh
#
echo "  Starting System Backups"
/bin/mt rewind > /dev/null 2>&1
sleep 3
/bin/mt status | if grep "No Additional Sense" > /dev/null 2>&1
then
        for FILESYS in / /usr /var ;
                do
                echo ""
                echo "Dump Command: ufsdump 0ucf /dev/rmt/0hn ${FILESYS}"
                echo ""
                /usr/sbin/ufsdump 0ucf /dev/rmt/0hn ${FILESYS}
        done
        echo "Backups Done."
        /bin/mt rewoffl
else
        echo "Tape Drive Not Ready!"
        echo "System Backups Aborted."
fi
exit 0
```

### Using dd to clone to another drive

Format and label the new drive, which should be identical in make, model and size.
Run “installboot /usr/platform/`uname -i`/lib/fs/ufs/bootblk /dev/rdsk/c1t0d0s0”
Then “dd if=/dev/dsk/c0t0d0s2 of=/dev/dsk/c?t?d?s2 bs=4096”

The 4096 seemed to be the optimal block size, balancing speed and accuracy. Since accuracy was paramount, the number was lowered a few notches just to be sure.

### Restoration from Tape

```
#!/bin/sh
echo ""
echo "Starting restore.sh"
mount /dev/dsk/c0t0d0s0 /a
cd /a
mt rewind
echo ""
echo "Restore / partition..."
ufsrestore rvf 1 /dev/rmt/0h
mount /dev/dsk/c0t0d0s0 /a/usr
cd /a/usr
mt rewind
echo ""
echo "Restore /usr partition..."
ufsrestore rvsf 2 /dev/rmt/0h
mount /dev/dsk/c0t0d0s3 /a/var
cd /a/var
mt rewind
echo ""
echo "Restore /var partition..."
ufsrestore rvsf 3 /dev/rmt/0h
mt rewoffl
echo ""
echo "Umount devices & fsck..."
cd /
umount /a/var
umount /a/usr
umount /a
fsck -y /dev/dsk/c0t0d0s0
fsck -y /dev/dsk/c0t0d0s3
fsck -y /dev/dsk/c0t1d0s0
echo ""
echo "Install Boot Sector to boot track..."
mount /dev/dsk/c0t0d0s0 /a
mount /dev/dsk/c0t0d0s3 /a/usr
cd /a/usr/platform/`uname -i`/lib/fs/ufs
installboot ./bootblk /dev/dsk/c0t0d0s0
cd /
echo ""
echo "Copy scripts back to / partition"
cp /tmp/*sh /a/
umount /a/usr
umount /a
echo ""
echo "Rebooting..."
echo ""
init 6
```

After this point, three implementation specific configuration files are transferred from an external source and the firewall daemons are restarted. At this point, the firewall is ready to be placed in service. If it is rebooted at this point, it will normally automatically place it self into the cluster. This can also be done manually with a single command.

## Complete Restoration Checklist from OEM Media

1. Power the firewall down.
2. Power the firewall back up.
3. During the Diagnostics portion of the boot, place the OEM Unix CD in drive.
4. The Operating System software would be installed at this point.
5. The Firewall software would be installed next.
6. The Load Balancing software would be installed third.
7. Copy configuration files and system custom scripts from CD.
8. Reboot.
9. Place back into cluster manually, or reboot.

## *Chain of Custody*

Logs are considered normal business records, and are routinely kept. A special-purpose server, with limited access, provides a repository for the logs.
The tapes are always treated as evidence as a matter of course, so a paper trail of their custody is kept, as well as efforts to maintain their physical security.

Firewall logs are written to syslog and hashed.
Syslog is copied continuously to the logging server.
Once a day, at 5 am, the logs from the logging server are backed up to 8mm DAT.
A member of the Security Team collects the tape daily, seven days a week.
An evidence tag (see Appendix) is created, stamped with a serial number, a description of the tape, date, time, person collecting evidence and it is bagged with the tape.
A log entry in the evidence log (see Appendix) is made for the item.
The evidence, in the bag with the tag, is placed in a locked cabinet, which is in a locked vault, which is in the data center.
Every month, the entire tape collection is moved to an secure off-site storage location.
After 7 years, the tapes are destroyed, in accordance with firm policy.

**The TWO-MAN rule is enforced at all times. At no time, is one person left alone with the evidence. The safe is also a two-man style safe.**

**Risks**
Overhead in tape storage and handling in onerous – This incident supports the decision to do this.
Latency in tape handling could be a risk if the data center was destroyed. If the tapes are vital to the investigation of the destruction of the data center, they have been lost – The need to rapidly be able to review logs locally appears to outweigh the risk. The risk is somewhat mitigated by another set of backups of the logging server moved offsite in a unsecured fashion.

## Forensic Analysis of the Firewall Data

1. A backup of the system was made to new tape, fresh out of the package. The backup of the backup was used for the examination.
2. At least two persons were present during the entire analysis.
3. All the forensic software was appropriately licensed.
4. The original computer was not available for the analysis, however, the purpose of the examination was to review the data itself.
5. The examination was done on a similar machine, unconnected to any other machine except a throwaway laptop. This was to avoid compromise.
6. A complete listing of all files was created, including their length.
7. The length of the files, as well as the Tripwire Checksums were made against a know good.
8. The access logs were examined, which are also shadowed to the logging server.
9. A comparison of the filesystems were made to the filesystems of a known good server was performed in order to produce a list of differences.
10. A hard copy was made of all apparent evidentiary data, including the file location, time, date, owner and checksum. The copy was serialized, signed by both parties and transferred to the Evidence Repository. Properly document comments and findings.

The conclusion of the analysis was the system was not compromised by any known technique.

## *References*

### Procedures

Organization Disaster Backup and Recovery Plan (SANITIZED by deletion)
Organization Security Policy (SANITIZED by deletion)
Organization Policies and Procedures (SANITIZED by deletion)
CERT Incident Reporting Procedure – http://www.cert.org/reporting/incident_form.txt

### Tools

Fred Cohens' Deception Toolkit – http://all.net/dtk/faq.html
The Coroner's Toolkit – http://www.porcupine.org/forensics/tct.html

### Applicable IETF RFC's

1244 Site Security Handbook. – J.P. Holbrook, J.K. Reynolds, 1991
(Obsoleted by RFC2196)
http://www.ietf.org/rfc/rfc1244.txt?number=1244

2196 Site Security Handbook. B. Fraser, 1997
(Obsoletes RFC1244)
http://www.ietf.org/rfc/rfc2196.txt?number=2196

### Custodianship

Field Guide for Investigating Computer Crime
http://www.securityfocus.com/focus/ih/articles/crimeguide1.html

Basic Steps in Forensics Analysis of Unix Systems
http://staff.washington.edu/~dittrich/misc/forensics/

IACIS Forensic Examinations Procedures
http://www.cops.org/forensic_examination_procedures.htm

IETF Guidelines for Evidence Collection and Archiving
http://www.ietf.org/internet-drafts/draft-ietf-grip-prot-evidence-01.txt

The Admissibility of Electronic Documents
http://www.forensics.com/resources/admiss.htm

Federal Guidelines for Searching and Seizing Computers
http://www.knock-knock.com/federal_guidelines.htm

## Books

"Incident Handling: Step by Step, Version 1.5" The SANS Institute, 1998
"Solaris Security: Step by Step, Version 1.0" The SANS Institute, 1999
"Windows NT Security: Step by Step, Version 2.15" The SANS Institute, 1999
"Telecommunications Fraud" Bob Wilson & Co, MCI Telecommunications Corporation, , 1994
"Internet Core Protocols" Eric Hall, O'Reilly and Associates, 2000
"Firewalls and Internet Security" William Cheswick and Steven Bellovin, Addison-Wesley, 1994
"Fighting Computer Crime" Donn Parker, John Wiley and Sons, 1998
"Web Security and Commerce" Simson Garfinkel and Gene Spafford, O'Reilly and Associates, 1997
"Defending your Digital Assets" Randall Nichols, Dan Ryan and Julie Ryan, RSA Press, 2000

## Book not used directly in this incident, but definitely worth reading

"Applied Cryptography" Bruce Schneier, John Wiley and Sons, 1996

## General Security Websites

Microsoft – http://www.microsoft.com.security
Sun – http://www.sun.com/security
Packet Storm – http://packetstorm.securify.com
Xforce – http://xforce.iss.net
Security Focus – http://www.securityfocus.com
Security Portal – http://www.securityportal.com
Nomad Mobile Research Center – http://www.nmrc.com
InDenial – http://archives.indenial.com
L0pht Heavy Industries – http://www.atstake.com
IT Security Cookbook – http://www.boran.com/security
Counterpane – http://www.counterpane.com
NIST Computer Security Resource Clearinghouse – http://csrc.nist.gov/policies/welcome.html

## Appendix 1 – Acceptable Use Policy

**AGREEMENT CONCERNING USE OF**
**ORGANIZATIONPROVIDED COMPUTER EQUIPMENT**

Fictional Organization, Inc.
Attn: Human Resources Department
111
Anytown, NY 00000

As part of our program of office automation, Fictional Organizationt, Inc. ("FicOrg") is allowing me use of certain equipment and software to assist me in performing my duties. In consideration, I agree as follows:

Compliance with all Copyrights. I have been provided with various software by FicOrg for use on FicOrg-provided computers. I understand that U.S. copyright laws and international treaty provisions protect this software and any accompanying written materials and that any reproduction is strictly prohibited. I will not lease, loan or transfer this software or written materials in any way. I will only use this software personally on the equipment provided. I understand that unauthorized copying or use of the FicOrg-provided software exposes both FicOrg and me to civil and in some cases criminal penalties.

1. Use of Additional Software. I will install additional computer software on a FicOrg-provided computer only with prior written approval from my manager and after I have notified ISG on the attached form. I understand that ISG is available to discuss additional software requirements by phone and may be able to provide guidance before I purchased additional software. I will acquire any additional software only from authorized sources and in compliance with all copyrights applicable to that software. I will provide evidence to ISG that I have obtained all required licenses for the additional software before installing it. I will observe all copyright restrictions applicable to the additional software. I understand that unauthorized copying or use of the additional software exposes both FicOrg and me to civil and in some cases criminal penalties.

2. <SANITIZED>

3. <SANITIZED>

4. Computer Data Property of FicOrg. I agree that all client data stored in my FicOrg-provided-computer is the property of FicOrg and may be examined by FicOrg at any time. I will treat all data stored in my computer with the highest degree of confidentiality. I understand that if I terminate employment with FicOrg, all client data must remain with FicOrg as required by law.

5. <SANITIZED>

6. Business Use of Computers. I will use FicOrg-provided computers only for business purposes. I will not install games or entertainment software on FicOrg-provided computers. I will not install any software that is malicious in nature.

I have read the terms set forth above and am signing this Agreement acknowledging my agreement to such terms, as well as my willingness to abide by any and al FicOrg policies and procedures and applicable rules and regulations of state, federal or regulatory agencies governing the use of personal computers and fax machines.

____________________ ________________________________________
Date Signature

________________________________________
Print Name

____________________ ____________________
Department Emp #

***Please send this original agreement to the Human Resources Department and maintain a copy for your file.***

## *Appendix 2 – Forms*

### Evidence Log (abbreviated)

| **Evidence Description** | **Unique Identified (Serial Number)** | **Signature of Collector** | **Evidence Tag Number** | **Date Collected** |
|---|---|---|---|---|
| Backup Of FW | 20000413001 | (Joe Schmuck) | 00-01 | 4/13/00 |
| | | | | |
| | | | | |
| | | | | |

---

### Evidence Custody Tag (abbreviated)

Item Description:

Reference Number:

Evidence Tag Number:

| Custodian Name | Date Received | Date Transferred | Purpose | Signature |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Incident Reporting Log

| Event Description | Event Reporter | Event Date | Event Time | Event Location | Comments |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

## *Appendix 3 – Sanitized IP Listing*

| Type of Network | IP Address Range |
|---|---|
| Internal, Private or "Red" Network | 198.168.250.0 – 198.168.254.254 |
| DMZ, Reduced Security | 198.168.200.0 – 198.168.249.254 |
| External, "Black" Network where addresses are owned by organization | 198.168.100.0 – 198.168.199.254 |
| Organization's ISP | 198.168.0.0 – 198.168.99.254 |
| Attacker's ISP | 192.168.0.0 – 192.168.99.254 |
| Attacker's Network | 192.168.100.0 – 192.168.199.254 |

| Host | IP Address |
|---|---|
| Affected Firewall (External) | 198.168.100.4 |
| Affected Firewall (Internal) | 198.168.252.202 |
| Unaffected Firewall #1 (External) | 198.168.100.5 |
| Unaffected Firewall #1 (Internal) | 198.168.252.203 |
| Unaffected Firewall #2 (External) | 198.168.100.6 |
| Unaffected Firewall #2 (Internal) | 198.168.252.204 |
| Attacking Host | 192.168.100.66 |

## Appendix 4 – Incident Handling Crash Kit

This entire set of tools is kept offsite in two bags, ready for flight. The exception is the dual-boot laptop, but all the software that is on that system exists on CD's in the kit.

Laptops

One Dual Boot Laptop with lots of memory (512M) and big hard drives (30 Gig)
Hard-drive #1 – Windows 2000 Professional (NAI Sniffer, Secure Shell, Sam Spade, NeoTrace, Firewall GUI, Time Sync Software, VNC, UltraEdit, Security Scanners, Virus Product Consoles)
Hard-drive #2 – Linux (Deception Toolkit, Coroner's Toolkit, tcpdump, nessus, netcat, nmap, gzip, and as many clean binaries such as ping, traceroute, whois, netstat and other basic OEM OS command line utilities)
Function: Recovery

Two (2) Linux Laptops
Hard-drive #1 – Linux (Red Hat)
Function: Throwaway, copying or auxiliary Sniffer

Media

- OEM Copies of all O/S (Windows 2000 Professional/Server/Advanced Server, Red Hat Linux, Solaris, HP/UX, AIX)
- Patches for all above systems
- Firewall Installation Media
- Copies of all software Tools installed on laptops
- Multiple DOS Boot Disks
- Bootable Linux CD
- Microsoft Windows Resource Kit
- Microsoft TechNet

Replication Tools

- Portable Parallel Port CD-Burner
- Portable SCSI Tape Drive
- Two-Hundred (200) Blank CD's
- Twenty (20) Blank Tapes
- Four (4) 9 Gig SCSI Hard Disk Drives
- Four (4) 27 Gig IDE Hard Disk Drives

Network

- 50 foot, 15 foot, 6 foot patch cables
- Cable Labels
- Two 8 port minihubs
- Cross Over Cables
- Receive Only Cable
- AUI Transceivers
- Fluke Network Diagnostics Tools

Tool Bag

- Hammer
- Screwdrivers
- Torx
- Diagonal Cutters
- Pliers
- Tie Wraps
- Tie Wrap Gun
- Misc Hardware
- Flashlights
- Compressed Air
- Isopropanol

Evidence Collection Aids

- Twenty-Four (24) Evidence Custody “Paks” (Tag, Forms and Envelopes)
- Digital Tape Recorder
- Magnetic Tape Recorder with 6 blank tapes
- Several packs of 9V, AA and AAA batteries
- One Dozen (12) Blank Notebooks
- One Dozen (12) Pads of Paper
- Hard Copy Contact List
- Hard Copy of Policies and Procedures, which include copies of all necessary forms
- Writing Utensils (Black Pens, Red Pens, Pencils, CD-ROM Market Pens, Highlighters)

Last, but not least

- Corporate Credit Card