Global Information Assurance Certification Paper

GIAC Advanced Incident Handling and Hacker Exploits Practical Assignment for SANS Security DC 2000

Option 1 – Illustrate an Incident

Johnathan F. Van Houten

The following incident occurred at this installation over a year ago, however, many points surrounding this issue are still under investigation by the Air Force Office of Special Investigation (AFOSI), and must therefore be extremely sanitized.

Every effort has been made to shed light on the major points as required for the practicum, without revealing material deemed 'sensitive' by that investigative office.

One of the unique difficulties in dealing with Internet based systems on a military installation is, interestingly enough, the first phase in incident handling; preparation. Politics play a major role, and often take precedence over safety and security. Systems are placed at risk of compromise – against the better judgment of contracted engineers – in order to facilitate an atmosphere of cooperation. Policy is enacted, but often waived or simply ignored. For instance, policy exists to ensure all machines are in compliance with CERT and AFCERT minimum required patch levels. Operating systems must be enhanced to a certain predetermined level and additional patches/hot fixes/service packs properly installed. Banners must be configured so any attempt to access a system is met with a forcefully worded paragraph, indicating the deleterious effect of unauthorized retrieval of information. Permitting 'weak' systems to exist in the unfriendly Internet environment, and disregarding important regulatory measures is the extent – albeit great – of the fragility in the preparation phase. Procedures followed during an incident, including this one, are fairly straightforward and for the most part, followed. A member of our Information Protection department noticed the potential intrusion as an odd probing from a system in our DMZ, to random IP's behind the inner perimeter firewall. He then notified me, and we tracked the probing to a server owned and operated by a tenant unit on this installation. Following established procedure, we monitored the server for signs of odd activity at strange hours. One key to our preparation plan is to ensure unauthorized activity to the best of our ability, before contacting the AFOSI.

Based on the information at hand, we contacted the flight commander and the installation Information Assurance office. The flight commander, in-turn, notified the squadron commander. While the Information Protection shop individual was appointed as the primary POC for this incident, we continued to work hand-in-hand to resolve the issue. We installed a 'sniffer' in the same subnet to monitor activity. We also gained access to the server in question and reviewed the log files. We were careful to never operate alone in this search – we always were together so that no one could claim complicity. We were also careful to only look at the system. Copies of the log files were made and then examined. It was during this phase we did indeed notice activity, both in a slight interactive probing of our internal systems, but mostly directed at outside organizations – both commercial and institutional.

We notified AFOSI and our immediate chain of command as to the live, unauthorized access we were now involved with. We notified the Air Force uplink, which manage the connectivity to all installations and requested that they examine their logs as well. Next we contacted the OSI office, and they instructed us to make back-ups of the system. We accomplished several, some to another hard drive we had 'slaved' in, and several to DAT tape. We did not use alternate methods – something which the SANS course taught – but that concept has been introduced into our procedure guide for future incident handling. Physical security of the system was increased. The machine already existed behind a cipher locked door, so the combination was altered so that only myself and the other IP representative knew the combination. While we did notify the organization of the incident, we did not permit their system administrator to gain access to said system. Policy dictates that the base level engineers will handle all incidents. The OSI also requested this.

Unlike the commercial world, the major command and the base felt no compunction to quickly restore operability of the contaminated server, nor to hurriedly replace said server with another of its kind. It was during this phase – containment – that the OSI arrived on-scene and took over the investigation, with the IP individual and myself working with them as liaisons. Their recommendation – and ours – was to take the data copied to backup, restore a new system to analyze, and place the old system back online with a monitor inline to record an inspect the intruder's network traffic.

With the system back online, being effectively monitored, we turned our attention to the cause and elimination of the compromise – what the SANS course describes as 'eradication'. We took the system we had built from back up, and attempted to retrace the intruders path. Fortunately, for us, most of the log files had never been modified. As it turns out, the system was rebuilt within the previous six months, with the administrator opting not to load the most current OS version, or the patch levels. All AFCERTS concerning security vulnerabilities, and required fix-actions had been disregarded. We ran several tools against the system to test for vulnerabilities, and it failed several.

Eradication was broad in scope. That system, and the information it contained never returned to active status. A scaled down version of the data they wished to present was moved to a more secure system. In this instance, the recovery phase simply did not occur. The tenant unit rebuilt all data, and the hardware was confiscated by the OSI – who continued to use such as a 'honeypot' of sorts, to track this individual further. All systems that co-existed in the same subnet as the compromised one, were thoroughly examined in similar fashion, and were found to be free of compromise. We did, however, use the backups to recreate the system as is originally stood in an effort to understand how the intruder compromised the system. We determined that there were several methods by which one could compromise the system. Since it was a default install of Solaris 2.5.1, it contained several vulnerabilities that were addressed in patch levels. The installation of apache also contributed to the potential for compromise, as it left cgi and phf vulnerabilities in place.

The follow-up report was drafted by the OSI, and then reviewed by each member of the team. The Information Protection representative and myself contributed to the report with information gleaned prior to the OSI's involvement, as well as thoughts we had during their investigation.

The OSI then updated the command structure during the 'out-brief' as to their findings and recommendations. Subsequent to their departure, we – the IP representative and myself – were involved in another meeting to discuss our installation's decision and summarize ways to avoid this in the future. We invited our command structure, the system administrator of the compromised machine as well as his command structure and the base legal department. The only topics discussed were the actual vulnerabilities, the methods used to determine the cause and effect of the compromise and what steps we should not take to ensure incidents such as this do not reoccur.

Since this investigation is ongoing, I will be unable to provide some specifics or screenshots, as they might violate the non-disclosure agreement I entered with the investigative officers.
I will, however, enter into as much detail as possible, and permissible.

No 'jump kit' was on hand; though we do have a checklist we locally manufactured which we follow during such occurrences. This checklist does contain a phone notification list. Up until the SANS course, I had not given much thought to developing an emergency action toolkit, though upon reflection, having one on hand would have made investigation more precise – relying less on individual knowledge, and more on proven concepts of investigation. I did have several of the tools, (Snort, Sniff, TCPDump, ls, lsof, ufsdump, dump) in binary form on a CD-R, though to this point, it was not policy to do so. This is something worthwhile that we are working toward.

The system in question was a default install of Solaris 2.5.1, on a Sun Ultra 20.
Our Information Protection representative first noticed the probing from the infected machine located in the DMZ – a zone just outside the firewall, but before the AFIN router – to various and seemingly random IP's within the secure perimeter. The probing consisted entirely of scanning commonly used and several specific uncommon ports. This was discovered using TCPdump and snort on, and around the compromised system. These measures displayed active scanning for specific services, such as SMTP (mail), HTTP (web), FTP (file transfer), POP3 (mail delivery agent), telnet and NetBios connections. One of the non-standard ports scanned were 31337, an obvious attempt to locate BackOrifice connectivity. All monitoring of these ports was handled at the Firewall, and TCPdumps were used to capture data requested from the compromised host. The command used was:

```
tcpdump –vv ip host  <compromised_hostname>  > output.txt
```

It was discovered that during the times of probing, access was gained to the system from an outside source. This was confirmed through the investigation of the router logs and correlation of the times of activity.

At this point we notified the OSI of the intrusion. Backups were made to an external hard drive, which was connected to the SCSI port of the Ultra 20. UFSDump was used to complete a full (level 0) backup of each individual file system to this drive, as well as to several 4mm DAT tapes. While the machine did have a DAT drive, we again, used an external SCSI DAT drive for the backup. We also disconnected the network cable from the server, until the OSI could arrive on-scene and survey the situation.

Once they arrived, the OSI assumed full control of the investigation. Not exactly a forthcoming agency, it was somewhat difficult to extract information from them during the crux of their investigation. It was made clear that the damaged system was being brought back online as a ‘honeypot’, or trap for the intruder, and that every piece of data being sent from and to the machine was being captured an analyzed on an inline server. I believe this machine was running a modified TCP packet analyzer, designed to trace back the original sender IP. This is all I am permitted to speak of this, as the investigation is still underway, though the server has been removed from service.

Backups were handled, as previously stated, through the use of a single backup method – UFSDUMP. External SCSI devices were attached to the system via SCSI ports. These devices included a Sun Ultra SCSI external hard drive (9.1GB), and an external DAT tape drive, also connected to the SCSI port. All dumps were handled at level ‘0’ for full backup. A separate command was used to ensure each file system was dumped to the destination. In the case of the tape device, a non-rewinding device name was used to ensure each file system was recorded sequentially on the DAT.

To verify a full and correct backup, n alternate machine was loaded from the backup using UFSRESTORE. First, information was restored back to a temporary directory, and then moved into place. This was accomplished with each backup, and each different device.

The only problem I see is with our procedure. The SANS course pointed out that several backups should be made, using different backup methods – most importantly using dd, a method of imaging the infected drive thereby ensuring a backup of ALL bits of the system. Since we used but one method, I would not consider us in compliance with proper procedure, and I am taking steps to add this method into our checklist.

Once it was determined that the system was indeed compromised, all access to the physical location of said system was withdrawn to anyone but investigative personnel. The system was quarantined, and disconnected form the network. Administrators who required access to the BIP (base information Protection) room to affect maintenance to their servers were escorted by a member of the investigation team.

The chain of custody in an organization such as this is fairly simplistic. The local investigators control the data and hardware until the arrival of the Air Force Office of Special Investigation team on the installation. Once they enter the investigation, all evidence is transferred to them, via a documented method involving a complete listing of all components of said evidence, and a formal transfer of control.

All backups were locked in a safe each evening, as well as all associated material. It remained at this location until the team withdrew from the installation.

Evidence included:

- DAT tapes used for backup (2 total, for two complete backups)
- DAT tape used to record the TCPdumps that we had accomplished
- External hard drive (also used for a backup)
- All of our notes – which were placed in the safe each night
- Our completed checklist
- The system itself.

The OSI team also retrieved some log information from the Air Force gateway controllers, though we, as local investigators, did not have access to that material.

The server in question did not have any normal backups, so none were available for the OSI to confiscate.

Executive Summary:

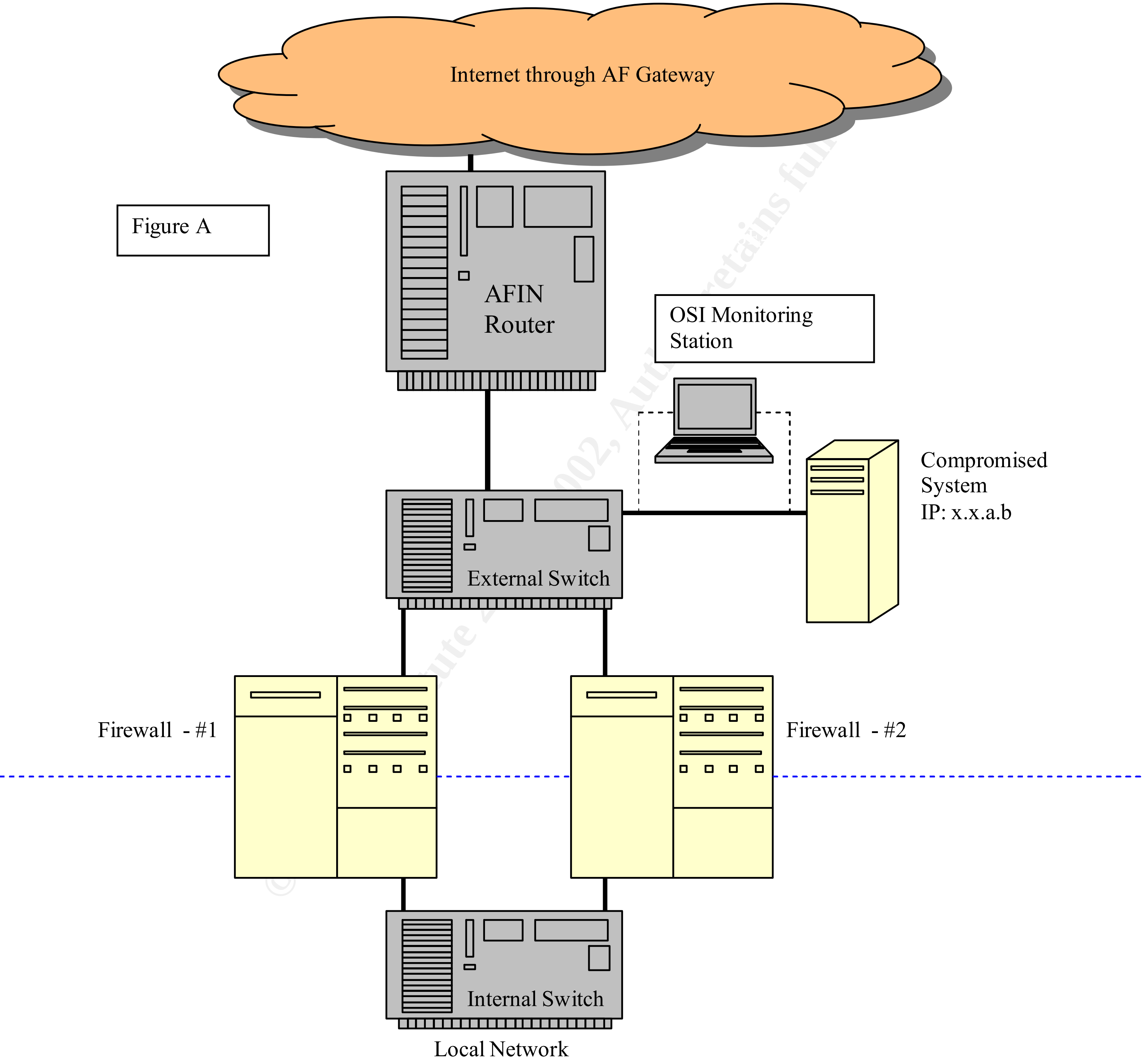
On or about (censored date) an intrusion was detected into one of the core systems, existing outside the base perimeter in the DMZ. It was found through the use of host-based intrusion detection schemes employed by some of our administrators and engineers. Information Assurance and the flight commander were notified of the potential intrusion, and further measures were set in motion. A determination of actual compromise was made after investigative methods employed to monitor traffic coming to and from this system revealed odd and unaccounted for activity. This was accomplished at the firewall using various network monitoring software packages – such as sniff and TCPDUMP. Further investigation revealed the source for this activity to exist outside the military domain structure. Again, the flight commander and IA were notified and the Air Force Office of Special Investigation was contacted. They directed both the IP representative and myself to isolate the system by removing the network connectivity, and to make multiple back ups of the system. We used external hardware - both hard drives and DAT tape backup units - to accomplish this with the UFSDump command. All TCP dumps were saved to DAT as well, and all media was locked in a safe, within the BIP room.
OSI arrived on station and assumed control of the investigation. The system was rebuilt on a different platform from the backups and subsequently examined for compromise information. The original system was placed back online, at the direction of the OSI, and included an inline monitoring system to record and analyze all incoming and outgoing packets of data. The object was to permit the intruder to continue (with limited capability) in hopes he might reveal information about himself, and his purpose. Meanwhile the newly created system was examined for vulnerabilities as well as for intrusion data both to find the method of compromise.
A determination was made that the intruder used vulnerabilities present in default installations of Solaris 2.5.1 that most likely permitted his entry. That system was summarily sanitized. It is highly recommended that all administrators follow procedure with regard to proper CERT, AFCERT, and manufacturer updates/security patches.

The AFOSI investigator, for further testing and analysis, confiscated all data and physical evidence. A final analysis and brief is expected, pending completion of the investigation.

The system in question was removed from service, and all functionality of tenant unit requirements are now being controlled at the base level.

Figure A. is a simplified diagram of the network structure, and may be used as a reference for this discussion.

Figure A


Internet through AF Gateway
AFIN Router
OSI Monitoring Station
External Switch
Compromised System IP: x.x.a.b
Firewall - #1
Firewall - #2
Internal Switch
Local Network