Global Information Assurance Certification Paper

Advanced Incident Handling and Hacker Exploits Practical

Meredith Lynes
14 Sep 2000

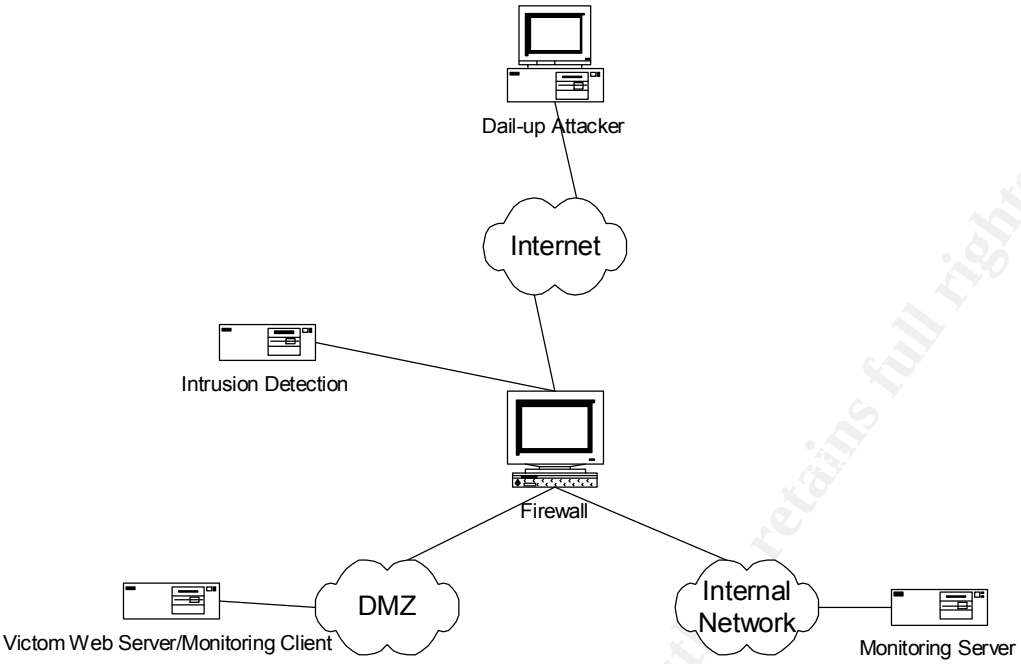
Executive Summary

On April 28, 2000 an unauthorized Internet user exploited a vulnerability of one of our publicly accessible web servers (here after known as Site 1)and replaced the default home page with one of their own design. The vulnerability exploited was the Microsoft Data Access Component (MDAC 1.5) for Microsoft Internet Information Server (IIS). Since Internet web access is permitted to this server the user was able to access and modify IIS files via the site firewall without alerting any of the firewalls monitoring mechanisms.

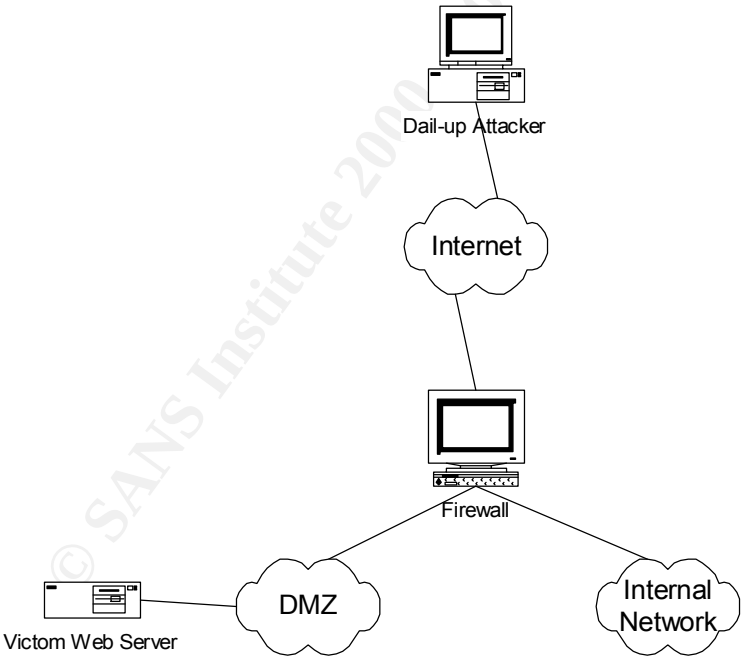
While our web monitoring systems did send an alert to indicate that the web page had been changed the operator simply cleared the alert. No action was taken until an anonymous phone call was received by an office in another geographic location. After notification the response team was able to isolate the vulnerability. The original web server was placed offline. Copies of the hard drive were made for study and the original was made available to law enforcement. The web services were restored after a complete vulnerability testing cycle using a spare web server. Total web service loss was under twelve hours.

Despite various advisories on the MDAC 1.5 vulnerability published by our Computer Incident Response Team (CIRT) in the days following this incident one week later another of our web servers was compromised albeit at another geographical location (Here after known as Site 2). No notifications were made. No log or system data was preserved by the administrators. It is believed that due to the similarity of the defaced page the same unauthorized user/users exploited the same hole. The second server was found to have the MDAC 1.5 vulnerability during an unannounced vulnerability scan after it was placed back in service. This was corrected.

The Network Engineering and Security Group issued a warning to Site 2. This warning stated that any further events which could have been prevented by following issued warnings and standard best practices would result in the loss of their right to operate a independent web server, and or the loss of network connectivity to the rest of the organization. This warning was issued in light of the fact that this was Site 2's second defacement within a year.



Site 1



Site 2

Preparation

Preparation is very often the most crucial step in any incident. In this particular case the difference between the two sites is readily evident.

General preparation Measures

Annual Information Security briefing for all personnel is required. All Internet accessible servers are required to be placed in an authorized and maintained Internet Point of Presence (PoP) unless a waiver is granted. A Computer Incident Response Team has been chartered, funded and staffed. The organizational CIRT publishes bulletins and recommendations on a regular basis. Annual training is made available to all Information System Security (ISS) personnel. Incident Reporting Forms are readily available. A 24/7 Incident hotline has been established. Organization wide vulnerability testing is done on a regular basis by the CIRT and the PoP personnel. All users must sign a user agreement form indicating their consent to monitoring. All perimeter router logs are regularly monitored. All internal backbone routers are monitored. Firewalls and Intrusion Detection Equipment has been placed at all authorized PoP's.

Site 1 Preparation Measures.

Site 1 is an authorized PoP with a large DMZ. A client/ server file monitoring package was installed on all Internet accessible web servers. Firewall policy is subject to review on a regular basis by a group of peers. Intrusion detection systems are in place. Firewall and Intrusion Detection logs are reviewed at least daily. System logs are maintained and reviewed daily. Firewall and Intrusion Detection logs are stored on a separate log server. While there is no written Information Security Policy network engineering/administration personnel attempt to conform to industry best practices. A clear cut out of band communication chain is well established allowing for timely notification of essential personnel. Regular backups of servers are maintained and tested. A set of backup's is maintained off site. Spare hardware is readily available. Personnel attend annual computer security briefs. Warning banners are in place on all systems. The emergency power shut off switches have been tested. The emergency generator is tested on a regular basis. A response team has been designated. The response team members at this site have similar jump kits. These consist of the following:

A cell phone and phone listings
A laptop with Linux running WinNT under Vmware.
Visors with blowfish encryption

As a group they share the following

A 5 port hub
Original installation CD's.
CD's with all current security patches for all OS's used on site.
New backup media
Various network cables.

Site 2 Preparation Measures.

Site 2 received a waiver to maintain a separate web server. A firewall is installed. No other data is available. The existence of a jump kit is questionable.

Identification

Site 1

The first indication of the incident occurred when the web servers file monitoring software alerted that the default.asp needed to be checked. This alert occurred roughly one minute after the page defacement. The alarm state on the monitoring server was cleared. The second indication of the incident was the receipt of an anonymous phone call stating that the web page had been defaced. The phone call was received by a representative located in the Boston area. He believed that the call was local. The recipient of the phone call immediately passed the information to the operator at the PoP. Roughly 30 minutes after the defacement the operator checked the web page. He then immediately called the system administrator to report the changed web page. The system administrator arrived on site and stopped web services. He then saved the defaced page and replaced it with the original. He also changed the admin passwords. At this time the calling plan was implemented and within 45 minutes all essential personnel were notified and/or in route to the site.

Site 2

Personnel checked the web page upon arrival to work and discovered the defacement. The system administrator was called to fix it.

Containment / Eradication

Site 1

Due to the time day and security measures already in place physically securing the computer deck was a moot point. No video equipment is authorized in that area nor is audio equipment thus note taking is all by hand.

The response team leader requested that the web server be unplugged from the network, and requested that no files on the effected server be modified. Since a spare web server was readily available it was decided to leave the original hard drive intact for evidence. One backup of the drive was made for study. I am not aware of what specific backup procedures where used in this case. Separate copies of the IIS logs where made to facilitate study by the CIRT.

A firewall wall log review produced little useful information. The only thing noted in the firewall was a well known site apparently taking a mirror of the defacement.

An audit of the Intrusion Detection System logs had negative results.

IIS log review was much more informative.

xxx.xx.xxx.xx, -, 4/28/00, 0:39:25, xxxxxx,webserver, xxx.xxx.xxx.xxx, 157, 32, 163, 200, 0, GET, /msadc/msadcs.dll, hr=80070057,CSoapStub::HttpExtensionProc,,

xxx.xx.xxx.xx, -, 4/28/00, 0:39:30, xxxxxx,webserver, xxx.xxx.xxx.xxx, 2891, 664, 1409, 200, 0, POST, /msadc/msadcs.dll, -,

These entries in the log were the first step in identifying what had happened. It and the next few log entries show the attacker probing the server. Additional log entries show the attacker checking for home.htm, home.html, index.htm, index.html.
A look up was performed on the IP using a third party service. It indicated that the user was coming from a dial-up located in the Boston area.

Several minutes later a similar pattern appeared
xxx.xx.xxx.xx, -, 4/28/00, 0:56:18, xxxxxx,webserver, xxx.xxx.xxx.xxx, 31, 32, 163, 200, 0, GET, /msadc/msadcs.dll, hr=80070057,CSoapStub::HttpExtensionProc,,
xxx.xx.xxx.xx, -, 4/28/00, 0:57:20, xxxxxx,webserver, xxx.xxx.xxx.xxx, 531, 1016, 1409, 200, 0, POST, /msadc/msadcs.dll, -,
xxx.xx.xxx.xx, -, 4/28/00, 0:57:23, xxxxxx,webserver, xxx.xxx.xxx.xxx, 15, 311, 312, 200, 0, GET, /Default.asp, -,

It was at this point that the default.asp was changed. These few traces were all that was available to work with to identify the user and the vulnerability exploited. A time line of events was drawn up based on log output.

00:33	Dial-up user tested web server for vulnerability
00:56	Dial-up user exploited MDAC vulnerability to replace defualt.asp
00:57	Monitoring system notified operator to check default.asp
00:58	Operator reset Monitoring console and cleared alert
01:15	Operator received notification of anonymous phone call about defacement
01:17	Operator paged Web Server system administrator
01:25	System Administrator spoke with operator and had him check page. Sys admin in route to site
02:06	Sys Admin on site and stopped web services.
02:15	Sys Admin saved defaced page
02:20	Sys Admin changed admin password and began the notification process
02:39	Team leader requested sys admin to unplug the web server from the network and asked him to not change any files.
03:30	All team members on site. Initiated backup's and log reviews.

After the basic log review and time line was drawn up, a quick look at the Microsoft Web site identified the MDAC 1.5 Vulnerability.

05:00	Team determined that the in house application developer's input was needed to fix the site, in order to retain all functionality.

Site 2

Site taken off line. Logging was not enabled on the web server.

Recovery

Site 1

After consultation with the in-house application developer the new equipment was loaded with original media and all available patches were applied. The data was restored from a known good back-up. A request was made by the Team Leader for a vulnerability scan of the server. The web server was scanned using NMAP, Whisker, and ISS scanner from the internal network and from the internet. These scans showed that the exploited vulnerability had been removed. Web services were restored at this time.

It was decided by the team leader to postpone the follow-up meeting until everyone had showered and been fed. It was clear that there were some issues with the process.

Site 2

System wiped and a complete reload of the OS from original media was preformed. Data was restored from backup's. The web server was then placed back in service. No testing was accomplished.

Follow-up

Site 1

At the initial follow up meeting it was determined that CIRT would issue an immediate flash advisory re-emphasizing the MDAC vulnerability. Several areas of improvement were noted.

1. While the monitoring software immediately alerted the operator that the default.asp had been changed, the operator simply cleared the alert and did not perform any further action until he received a phone call indicating that the web site had been defaced. It was decided that operator training needed to be updated to include proper procedures for the monitoring software package.

2. It was determined that the notification process was somewhat faulty. In the future the site response team will be notified at the same time as the system administrator.

3. A short training session regarding Incident Handling procedures needs to be developed to focus on system administrators duties and responsibilities.

4. A general training program needs to be developed regarding Incident Handling for all personnel.

Since the original server was still intact it was decided that law enforcement should be notified, with the CIRT acting as the main point of contact. Arrangements were made to properly secure the server pending any legal action. These included storing the server in a secure location and placing seals on the server. Copies of all notes where made and the originals where signed, dated and placed in a secure location.
The meeting was adjourned with the Team Leader taking responsibility to ensure that all proper paperwork regarding this incident was completed in a timely fashion.

Site 2.

No follow up meeting was held. CIRT notified of the incident.

Lesson Learned at an Organizational Level

The Network Engineering and Security group reviewed these events at their weekly meeting. This meeting took place one day after the events at Site 2.

It was discovered that the original CIRT advisory on the MDAC vulnerability and corrective actions needed was originally published in July of 1999. This advisory had been sent to all Information Systems Security personnel.

Since this was the second defacement of Site 2 for which no information on the incident was available for review, it was decided that a strong stand on the part of the group needed to be taken.

It was decided that training on incident handling was a universal need throughout the organization.

CIRT informed the group that Law enforcement would not be pursuing this incident. Although the evidence was preserved properly at Site 1 with out any evidence from site 2 the dollar value of the case did not warrant any further action on the part of

law enforcement. It was decided that in the future law enforcement would only be called if the dollar value of the incident was clearly above their requirements.

The topic of web server location and control was discussed. It was determined that positive control of all Internet accessible servers must be maintained. CIRT was charged with locating any and all unauthorized sites.

It was decided to develop a forum in which geographically separated ISS personnel could effectively communicate. An intranet accessible secured bulletin board was proposed and accepted as a solution. An implementation deadline of one week was placed on this resolution.

Some type of accounting measures must be put in place to ensure that security patching is done in a timely manner.

The following findings regarding the sites concerned were released to ISS personnel.

Site 1

Impact: Web server maintaining the web page HTTP:\\our server was infiltrated. This forced the Web site to be down for approximately 12 hours and loss of the use of the web server till a full investigation can be completed. Currently the site is running on a backup web server.

Action: The CIRT has contacted the administrative, security network staffs, and law authorities and advised them to take action as deemed appropriate to protect assets and resources.

Notification: Advised personnel. Notified the FBI.
Recommendation: Block IP Range for 180 days. If no further activity is noted during recommendation period and the ISP has taken appropriate action to correct the situation, CIRT will coordinate with the network staff to discontinue action on controlled security systems.
Follow Up: CIRT will continue to coordinate with network staff and the FBI until a proper resolution and conclusion can be reached. Actions to preserve the affected system have already been initiated and will be used for further analysis as soon as the data images are made available to CIRT.

Findings: The individual(s) performing the System Intrusion gained access to the web server using the MDAC 1.5 vulnerability in NT 4.0. This vulnerability and necessary corrective actions had been previously reported to appropriate individuals by the CIRT and Information Systems Security personnel in July 1999, when it was published by Microsoft.

Site 2

Impact: Web Server was infiltrated, publicly accessible web pages defaced, and a possibility of Trojan programs placed on compromised system.

Action: The CIRT has contacted the Coast Guard administrative and security network staffs and advised them to take action as deemed appropriate to protect assets and resources.

Notification: Advised personnel.
Recommendation: Perform a top down review of security practices and procedures by Site 2. Have all Site 2 system administrators, network administrators, and Information System Security personnel review published ISS procedures for Incident Handling, which is located at the following URL.

http://www.intranetwebserver/cirt/incidentsteps.htm

Perform a reload of the compromised web server from a backup prior to the attack to ensure no Trojan programs are on the system. Have Site 1 Web Administrators evaluate Site 2 publicly accessible web pages to determine if they should be hosted on Site 1's web servers, as per standards.

Findings: All System Administrators, Network Administrators, and ISS personnel need to take time and review the ISS Incident Handling procedures. This could lead to better recording of events, proper logging of systems, notification of CIRT / ISS in a timely manner, and preservation of the crime scene. In this case, the lack of evidence makes investigation of the event impossible, and law authorities can not be used to assist the CIRT in the tracking and apprehension of the individual(s) responsible. Since the attack was made by the same group as the last attack, the CIRT can only assume that it was done using the same exploit that allowed the group, to deface the Site 1 web server the week prior.

The following statements regarding overall organizational Information Security Readiness and procedures were released by the group.

The recent second successful hack of the Site 2 web Server and the FBI criminal investigation of the Site 1 web server hack brings the issue of web site security to the forefront. CIRT is compiling a list of organizational web sites from simple web search engines. There are more than we imagined. It is becoming clear that we are a target for at least one hacker and most probably more. Sites such as:

Deleted
Deleted
Deleted

and more are outside the organized protection of and security review provided the "official" sites run at Site 1. While Site 1 may not provide a "hack proof" environment, it does have security measures and daily security reviews in place. These other sites do not. The recent contrast between the Site 1 hack and the Site 2 hack provide a case in point.

Site 2 rebuilt the hacked system after they detected the hack, thereby erasing vital evidence in a federal crime (that in itself is a federal crime, but we won't go into that); Site 1 maintained evidence and is cooperating with the FBI. Security logs are maintained for months at Site 1 so tracking hacker crimes is easier. No such logs are maintained or reviewed at other sites. Site 1 works directly with CIRT on a regular basis and is aware of the ever changing security environment on the Internet. Security scans are performed at Site 1. Security log reviews are done daily from Site 3 (covering all authorized PoP's). Outside sites are not scanned and their personnel are unaware of the latest security measures, policy, or rules of criminal evidence.

It is time to take security seriously for all organizational web sites and operate in a professional (and legal) manner. Hackers could change information on the web pages above which could mislead the public and do harm to the public and our missions.

Recommended Policy issued by the group to Management as a result of these events:

No Organizational program or entity shall maintain an Internet accessible Web Site outside the confines of Site 1. Exceptions to this policy MUST obtain a written waiver. Justification for the waiver MUST strongly address security issues and demonstrate a technical knowledge of the issues involved and the legal ramifications of actions taken in the event of a security breach. Any program maintaining a web site under waiver which fails security scans and/or is broken into 3 separate times (each after remediation) shall permanently forfeit their waiver. Any site under waiver which fails to maintain rules of evidence in the event of a security breach shall permanently forfeit their waiver.

Status

The bulletin board for ISS personnel was implemented, however it has remained under utilized to date. Actions must be taken to remedy this.

An Internet Security Briefing was held at the annual ISS conference with an emphasis placed on training users. Plans include expanding the time spent on Incident Handling Procedures and Users Awareness.

Formal Policy is still non existent.

Notes

The events presented occurred within my organization, however I was not able to be present at Site 1 due to geographical issues. I did however take part in the after action meetings via telephone.

All information in this report has been sanitized to the standards of my organizations. I am not able to provide any more detailed information regarding network set up then is on the diagrams below. I am also unable to provide any screenshots of effected systems, for several reasons. 1. The defacement would unsanitize the whole thing. 2. I was not present at the investigation and this entire report is based on interviews with the Response Team, the CIRT and my attendance of the after action briefings. The only event left out of the time line is the 0230 courtesy call I received letting me know that Site 1 had an incident. I did communicate with the Response team during the investigation and offered suggestions on how to proceed. I am currently spending a great deal of my time attempting to get a formal security policy pushed through management. I believe that this will help deter future sites handling incidents in the manner of Site 2.