Network and System Planning - How to Reduce Risk on a Comprimised System

Brent Maley

Network and System Planning – How to Reduce Risk on a Comprimised System
Brent Maley
Sept 18, 2001

When most system administrators configure their computer system, most effort is put to protecting the system from an attack, hotfixes are installed, and common vulnerabilities are removed. However, hackers are constantly finding new holes in Operating Systems, and services being run on the computer systems. Even a well-hardened system can become subject to an attack once a new threat has been found and the hole is not immediately patched.

This paper is going to highlight the Code Red Worm as a specific example of an attack. It will demonstrate how a network can be setup to help limit exposure to it and other similar attacks. It will also look at how a network can be designed to reduce the chance of it being infected, and then go a step further to show how to limit the risk associated when one of the systems has become infected. It will touch briefly on hardening, as well as network and firewall configuration. While it will relate to most any attack, I will look specifically at the Code Red Worm as an example, showing how it infected systems and what could have been done to limit its ability to attack and them, and show how the systems could be setup to reduce the risk of exposing their data if they have been compromised.

What the Code Red Worm is:

CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL

> The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a webserver can be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the indexing Service described in CERT advisory CA-2001-13.[1]

Cert Advisory CA-2001-13 Buffer Overflow in IIS Indexing Service DLL

> There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victims system.[1]

The original bug, an issue with the indexing server, was posted as an advisory on June 19, 2001. (CA-2001-13) Less than one month later, an advisory was released for an attack, the Code Red Worm, on July 19, 2001. (CA-2001-19) This worm took many

companies completely by surprise even with the heightened awareness brought on by the media.

The Code Red worm is similar to many of the attacks, which have begun to hit the Internet. These attacks are able to circumvent a firewall. The attacks do not directly attack the firewall itself, or attempt to go around it, but instead, choose a known allowed port and use it just as any normal traffic might use. In the case of Code Red, it went through the firewall on Port 80 as standard HTTP traffic. Stopping an attack like this directly with a firewall is limited since most firewalls are configured specifically to allow HTTP traffic to the web servers. Additionally most firewalls, even with application scanning will not stop most buffer overflow attacks. Unfortunately many small understaffed IT departments rely to heavily on their firewalls to protect their systems not realizing the limitations firewalls have.

After connecting with a web server, the worm, would attempt to infect the web service if the systems had not been patched or hardened to not allow the infective action, thereby causing the server to become infected. Once a web server became infected, it started spreading the worm to all the web servers within reach. This was achieved by randomly attempting to open web connections to other Internet addresses. If it managed to hit an IP address with Port 80 open, the server would try to infect it, thus starting the cycle over from a new server.

While the original Code Red Variant 1 and Code Red Variant 2 did not create backdoors, or compromise data, there was speculation that the Code Red Variant 3, could pull data from databases that were connected to the infected web servers and therefore to the Internet. Additionally it would not have been difficult to modify the original worm to install backdoor programs such as BackOrifice or RootKit on the infected servers.

When you look at attacks, you need to consider two different things.

1. How do you prevent the attack from happening?
2. How do you contain the attack once you have been compromised?

How to Prevent an Attack

The easiest way to prevent a system from being compromised is to keep up on all security patches required for the system, and to harden it as best as possible depending on the applications required to be running on the server. This includes only running the minimum necessary applications needed on a server. However unfortunately for some small shops this would mean that the system administrator might never get to leave the office, even at larger companies with large IT staffs, missing a critical patch is always a problem especially in complex network environments where you have thousands of servers. Eventually even the best managed systems have the potential for being comporomised, so consideration needs to be made to reduce the complexity of the network.

Limiting Exposure on a Network

The first way you can limit exposure to attacks on your network is to define what services each server and workstation needs to be running. Limit these services to the required services only. The Code Red Bug overwhelmed many networks, not because they had one or two web servers spamming their networks, but because employees had installed the web services on their own workstations. This caused many IT departments to have hundreds or thousands of servers that were infected instead of just a few. While in some circumstances people require web servers on their workstations for development and testing, in most cases these provide no functionality other than creating a potential jump off point for a worm or other hostile attack. It gets extremely difficult for an IT department to manage large numbers of workstations, by eliminating some services off these devices it lowers the chance that a patch or fix will get missed.

Once you have determined what services you require on a server such as Web or SMPT etc, you can then look into hardening and locking down those applications in addition to the Operating System. Many applications come out of the box from Microsoft and other developers with un-required often-unused services. Some services that can be part of an application such as IIS can be used to a conduit for an attack against the system. For instance, when you install IIS 4.0 just to have a web server if you are not careful, it will install an SMPT, FTP, Transaction Processor, and Indexing Server in addition to the web services. The Indexing Server, which is compromised by the Code Red Bug, is one of these.

> *As part of its installation process, IIS installs several ISAPI extensions. These are dynamic-link libraries (DLLs) that provide extended functionality. Among these is Idq.dll, which is a component of Index Server (known in Windows 2000 as Indexing Service) that provides support for administrative scripts (these are Internet Data Administration, or .ida, files) and Internet Data Query (.idq) files.*[2]

By just eliminating the links to the idq and ida files, you could have eliminated the risk of the Code Red Worm without even patching your server. However even if you are not currently at risk, it is always advisable to install patches and hot fixes for known security issues since upgrades and installs could change the settings on your server re-enabling services that you had previously turned off. Additionally even though the Code Red Worm only affected Windows Servers directly, both Linux and UNIX servers as well could have a similar attack targeted against them.

You can find hardening documentation at various places on the Intranet. You can find this information on SANS site at the following addresses.

> Win2000 http://www.sans.org/infosecFAQ/win2000/win2000_list.htm
> Windows http://www.sans.org/infosecFAQ/win/win_list.htm

Hardening your servers and workstations is just the first step in preventing an attack from breaking into one of your systems. It limits what an attacker will be able to utilize.

However, some programs will still be accessible such as the WWW service on a web server. It is important to keep up with patches and hot fixes on these services. Advisories can be seen for new attacks on the CERT website, http://www.cert.org/. Additionally when you are hardening your servers, if you have a large number of them, make a checklist to ensure you do not forget some of the small things such as setting a strong password for the local administrator account. Remember no matter how hard you harden a device; if so to say you leave the keys under the mat in front of the door, the hackers will be able to just walk right in.

Additionally hardening workstations and servers will only work as long as you have complete control over the environments of the systems themselves. An IT department can effectively harden all of their servers and workstations, only to have a user reinstall a program wiping out all of the effort made to secure the system opening it up for attack once again. The risk of this can be reduced by limiting the ability of users to reinstall programs on their computers, however this becomes difficult to manage in complex environments were users require high levels of system access. A well defined change management policy can help prevent issues on controlled servers, because it can provide a path for notification to the required parties who maintain the servers. Notification that an upgrade is being perfomed will allow the appropriate people to determine if they might need to reapply portions of the hardening and lockdown procedures.

Host Based Intrusion Detection Systems

One area you can look at to help reduce the risk of being compromised is by adding a Host Based Intrusion Detection System. This is an area, which has changed dramatically in the past several years. In the past most Host Based IDS systems were more reactionary, and they did little to stop an attack from occurring generally their purpose was to spot an attack that had occurred, by changes made to the system, then notify an administrator via an alert, or run a pre programmed action. While this is somewhat effective, this still creates short periods of risk for attack that are seen, and does little to stop an attack you are currently not watching for. An example of this would be Symantec's Intrusion Detection Agent. While this program could be setup to watch logs, and file systems for an intrusion, it would not actively prevent an intrusion from taking place.

However, several new products have recently been released to the market; Sanctum's AppShield and Entercept's Web Server Edition. These new Host Based IDS Systems are taking a new approach to Host Based IDS. They have been built to protect specific services; such as web services, which are some of the more commonly attacked services. These new programs are designed to review the traffic being sent to the server and prevent any suspect traffic from reaching the actual application service itself. Looking at our example, the Code Red Worm, this would have been stoped, even without patching the systems or removing the links to the indexing dll because the IDS system itself would have reviewed the HTTP session, have seen that it was a buffer overflow attack, and stoped the session from reaching the web application.
Sanctum and Entercpet's products can be seen at the following addresses

http://www.sanctuminc.com/solutions/appshield/index.html Sanctum's AppShield
http://www.entercept.com/products/wse/index.asp Entercept's Web Server Edition

It is important to remember though that even having installed one of these programs, you will not completely secure your system. Thes programs look for suspicious traffic which falls under known attack patterns, similar to the way many Network IDS systems work. As hackers become more creative in their attacks, these systems to have the potential to become at risk, and administrators must ensure that these systems are also kept upto date with the latest signature files provided by the companies. Additionally these programs are can be costly so are not available to many small IT shops on a tight budget.

Limiting Exposure on a Compromised System

Hardening a server and installing hot fixes are the best way to prevent getting your network compromised. Nevertheless, they cannot prevent all of the unknown attacks that hackers will come up with in the future. Eventually most any server will have a situation come up where it could be hacked or compromised. This does not have to come from the outside; an employee or user, installing software could intentionally or unknowingly compromise your network or servers by installing a program that has a security hole, or which contains a backdoor.

The second part of limiting exposure is setting up your network properly incase you are compromised. This can be best done by setting your network up in a DMZ configuration, and having a highly defined rule-set on your firewall limiting each service. Before you can begin to setup the firewall rule set, you need to have a Security Policy. It should have not only sections for detailing what type of external traffic is allowed into the network, but also an Acceptable Usage Policy for what type on internal traffic is allowed out. Having these policies defined before you being working on the rule set helps eliminate issues when you begin to block various services.

When you are looking at protecting your data, people are usually relatively good about detailing the external traffic coming in. Most times this is the easiest to define such as allowing external traffic into your web server, or allowing mail into your mail server.

Internet to DMZ (Servers)

- SMTP
- HTTP/HTTPS
- FTP

DMZ to Internet

- SMTP

Corporate Intranet to DMZ – DMZ to Corporate Intranet

- SMTP

Corporate Intranet to Internet (Workstations)

- HTTP/HTTPS
- FTP
- Telnet
- ICMP
- ICQ/AOLChat

The above lists are typical for what many smaller companies might be allowing in and out of the network. While this list certainly does not cover the entirety of what a company will allow either into our out of their network, it does cover a small range of what could be allowed.

It is important if you are trying to limit exposure to attacks when you configure your firewall to look at servers and workstations differently. In general, workstations need rights to go out of the network, and servers need certain services allowed into the network from the Internet such as HTTP. Servers in most cases should not be allowed out onto the Internet. While this can make it more difficult to download hot fixes and other patches to a server, it reduces their ability once compromised to start sending data out.

If a larger percentage of web servers had been in a DMZ configuration where they were unable to initiate an external connection, even though infected, they would be unable to continue spreading the infection. Additionally, setting up a Firewall so that it allows only incoming http connections to a web server, and that the web server cannot initiate any connections going out, you drastically reduce the ability for a worm to install a program on your system that will allow it to compromise your data. This also prevents the worm, as in the case of the Code Red Worm, from spreading. In the case of the Code Red Worm, the worm spread almost unchecked across the Internet. One of the reasons being that once a server was infected; it infected other servers.

Setting up a network with a simple DMZ configuration, as shown above would have reduced the impact of compromised system on your network. If a webserver had been compromised in the above configuration, both the data on the web server would be secure since it could not open connections out of the DMZ, either to the Internet or to the corporate network. Both would have been secured since the infected web server would have no access to open any out bound connections, except for SMTP. This would shield unpatched webservers and other applications running on the internal intranet. It also would have stop any worms or other applications from using your server as a jump off point to attack another system further down the line.

Lessons Learned

Part of the reason the Code Red Worm spread so fast was that there was little in the way preventing it from going forward. While the immense numbers of servers and workstations within a corporation, many utilizing personal web servers or other applications, caused some of the problems, the wide range of this problem soon became apparent. Although initially thought to be the main offender, corporations were not the only group that had their systems open to the Code Red Worm. It became rapidly apparent after a few days, that a large number of the infected systems were home users, in general running perpetual connections to the Internet connecting through DSL or on a Cable Modem, however even dial-up users were at risk. Home users systems unfortunately make excellent targets since they are less likely to have anyone monitoring their systems. It is also a good chance that these home systems do not require a password to login or connect to any other system in their "network". Many home users have also been negligent in taking the time either to harden their home systems or to purchase a home firewall such as:

BlackICE Defender by NetworkIce: http://www.networkice.com
Symantec Desktop Firewall by Symantec: http://www.symantec.com
ZoneAlarm by Zone Labs: http://www.zonelabs.com

Most everyday users are unschooled as to the programs and services running on their computers. Many mistakenly think that they need to be running a web server in order to surf the web. As operating systems become more complex, and programs exercise more control over our lives, the lack of security on Internet connections and systems connected to the Internet will become an increasingly serious issue. The proliferation of worms and viruses will eventually push home and corporate security to the forefront of awareness for everyone on the Internet.

References

1. CERT Coordination Center
   http://www.cert.org/advisories/CA-2001-19.html
   http://www.cert.org/advisories/CA-2001-13.html

2. Unchecked Buffer in Index Server ISAPI Extension can Enable Web Server Compromise, Microsoft Knowledgebase Article (Q300972)

3. Rob Lemos, *Virulent Worm calls into doubt our ability to protect the Net*, July 27, 2001
   http://news.cnet.com/news/0-1003-201-6658647-0.html?tag=tp_pr

4. Chris Klaus, *Code Red: Is the worm a slug?* July 31, 2001
   http://fyi.cnn.com/2001/CAREER/trends/07/31/code.red.klaus.focus/

5. Paul E Proctor, *Hardening Windows NT Against Attack*, January 1999
   http://secinf.net/info/nt/hard/hard.html

6. Phillip Cox, *Hardening Windows 2000*, May 25, 2001
http://www.systemexperts.com/win2k/hardenW2K12.pdf

7. Joe Rudich, *Network Lockdown*, August 2001
http://www.computeruser.com/articles/2008,2,2,1,0801,01.html

8. Lance Spitzner, *Building Your Firewall Rule Base*, January 26, 2001
http://www.enteract.com/~lspitz/rules.html

Last Updated: February 20th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
SANS Riyadh February 2019	OnlineSA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced