




The original author of this course is Randy Marchany. Some technical information has been added from Mary Chaddock's GSEC practical assignment.




Introduction

- ◆ This presentation is designed to give you a brief overview of the top 10 most critical Internet Security threats.
- ◆ These aren't the only threats...*just the most common at the moment.*
- ◆ Hopefully, we'll eliminate these threats and create a new list next year.

2

This short course is designed to make you aware of the Top Ten successful attacks that have been used against sites in the past couple of years. Hopefully, by addressing these vulnerabilities first, we eliminate some of the known holes present at most sites. These are NOT the only security weaknesses, but this should give you a better handle on securing your systems.




Why Are We Vulnerable?

- ◆ Computer systems and programs have become more complex in the past 25 years.
- ◆ Quality control hasn't been able to keep up due to market pressures, programming skill deficiencies, etc.
 - Most of these programs/systems are based on code that was never intended to be “production” quality. They were “proof of concept” programs that became the basis of production systems.

3

Since there was no central UNIX development group, it was up to the individual programmers to check their code. Some did and some didn't. Others wrote programs with the expectation that this was a temporary thing only to find out years later that the programs were still around. The UNIX r-commands are an example of this. They were written as a temporary measure while the real telnet and ftp programs were being written. They're still around today and have been the cause of a number of break-ins.

Quality control is a real issue when it comes to determining if a piece of code is “secure”. Most companies simply don't have the time to check ALL the possibilities because of a number of reasons.



So Many Systems, Not Enough Time.....


- ◆ 2.3 million hosts are connected to the Net each month. There aren't 2.3 million sysadmins. Something has to give....
- ◆ Unfortunately, it's the sysadmin.
- ◆ Not enough training, too many conflicting demands on their time.
- ◆ The Prime Directive: Keep the system up!
- ◆ Patch the system? When I have time....

4

There aren't a lot of system administrators with a wide range of experience in the job market. The LevelOne course that you will take as part of this course sequence is an attempt to address this weakness. (*Editor's note: The LevelOne Security Essentials course is available through SANS' GIAC Training and Certification program. – JEK*) There are a number of colleges and universities that are developing a System Administration set of courses but these courses will address the long-term shortages only. Most sysadmins don't have the time or luxury to get official training. Their training is by apprenticeship or OJT.

Some vendors are now advocating the centralization of systems...this is what used to be known as the "mainframe" model ☺. The Sun Sunray terminal device is an example of this return to the past. It doesn't solve the sysadmin issue though – a poorly trained sysadmin of a big system is just as bad as 50 untrained sysadmins in the field.

The Prime Directive forces sysadmins to cut corners sometimes and this is where problems can compound themselves into serious vulnerabilities.




Hacking = Rocket Science? Not!

- ◆ Any good hacker can write the attack tool. The real skill is making so easy to use that a CEO could launch the attack.
- ◆ There are lots of hacker WWW sites where you can get these tools. These sites try to outdo each other by designing the best, baddest, user-friendly site.

5

A small minority of hackers have the technical expertise to write some of the attack tools commonly in use. Their view is that anyone can write an attack tool, but the art comes in how you package it and make it easy to use. Sites like www.rootshell.com, www.insecure.org, <http://thc.pimmel.com>, www.securityfocus.com and others are examples of where one can download a wide variety of attacks tools. These sites make it easy for anyone who knows how to use a browser to get these tools. Fortunately, most of these people don't know much more than how to use a browser but that will change soon.

Use your favorite search engine and lookup "NT Hacking", "Solaris hacking", "Netware Hacking", "Windows 2000 hacking". You'll be surprised at the number of sites that have readily available tools.




Why Are the Attacks Successful?

- ◆ We didn't close all the doors because we're too busy doing "real" stuff.
 - If the hackers got caught, we didn't punish them. It would be too embarrassing to admit we got hit. Our Incident Response Plans were inadequate.
- ◆ The attack designers studied (cased) the target code carefully.
 - A lot of attacks are based on Buffer Overflows.
 - Example: a program expects 80 input characters max. You give it 5000 characters. How does the code handle it?

6

A great reference paper that describes the buffer overflow attack is Dildog's "The Tao of Windows Buffer Overflow". It's available at www.cultdeadcow.com. The basic weakness is poorly designed code. Coders didn't spend enough time debugging all possible error conditions. Dildog's paper is easy to read and a must for anyone who used Microsoft products.




Some Pointers About the List

- ◆ Each item in the list is divided into 4 parts
 - A **description** of the vulnerability
 - The **systems affected** by the vulnerability
 - A **CVE number** identifying the vulnerability
 - Some suggested **corrections**
- ◆ What's a CVE number?
 - CVE = *Common Vulnerabilities & Exposures* reference number that is used to uniquely identify a vulnerability.
 - It's like the Dewey Decimal #'s that are used in the library. You can go to any library and find the same book using the same Dewey catalog number
 - CVE's does the same for vulnerabilities.

7

When you look at the Top 10 document, you'll find it's organized into the sections listed above. The Mitre Corporation has initiated a project to classify the vulnerabilities using a code called a CVE number. Think of the CVE number as a library catalog number. It's a simple and effective way to ensure that a vulnerability definition means the same thing to different people.

If vendors list the CVE that their particular tool addresses then this gives us a way to compare products and make an intelligent purchase.



Item #1: BIND

- ◆ All Internet systems have a hostname and an IP address.
 - Every home is known by its address and who lives in it. “hey, is that Randy’s house?” “Yeah, it’s at 24 Main St.”
 - “Randy’s house” = hostname
 - “24 Main St.” = IP address
- ◆ BIND (Berkeley Internet Domain) maps hostnames to IP addresses.
 - It’s the set of “phone books” of the Internet.

8


In the old days, internet hosts were listed in a file called `/etc/hosts`. This wasn't a big file (remember, it was the early years of the net) and when a new system came online, its hostname and IP address was added to the file.

You can see that with 2.5 million new hosts added to the net every month that this file is not practical to maintain. Forget updating it, try searching for something in it! Then you have to make sure EVERYONE has the same copy or else some sites won't be able to connect to other sites.

The Domain Name Service was designed to alleviate this problem and make hostname and IP address maintenance more manageable. The `.com`, `.gov`, `.mil`, `.edu`, `.net` and `.org` names that are so familiar to us evolved from this DNS project. The concept was quite simple. Since the Internet is a collection of networks, we would designate a set of machines to act as nameservers for their individual nets. Every network would have at least one nameserver to handle the mapping for its network.

The name of the process that runs BIND will be named or `in.named`. Named is normally run as a daemon. Use `ps` to determine if named is running.

```
(Solaris) $ ps -edf | grep named | grep -v grep
```

Item #1: BIND

- ◆ Every network needs a couple of systems that run BIND. They're called **nameservers**.
- ◆ Old versions of BIND have security holes. The nameservers aren't always up-to-date. They were when they were installed but that was years ago. It works so why fix it? Right? Wrong!
- ◆ **The Danger:**
 - Hackers get full control of the nameserver and can use it for anything they want.
- ◆ **A Solution**
 - Make sure your version is higher than BIND 8.2.2 patch level 5


9

Improperly configured nameservers can give a hacker all the names and IP addresses of internal systems. In some cases, this information can also include the OS and machine type. Hackers armed with this knowledge can then search the net for the specific attack tool and then target a specific machine inside your net.

You should ensure that BIND is at current patch levels and versions.

Nameservers are fairly static systems and so aren't checked as frequently as a production or development system. As a result, a hacker could break into the system and the activity usually isn't noticed until someone from the outside reports an attack originating from the nameserver system.

If your system is running named and is NOT a nameserver you should turn it off:




Item #2: CGI Scripts

- ◆ CGI = Common Gateway Interface
- ◆ It's the language that programmers use to display and read your input to a WWW based form.
- ◆ Not everyone knows how to use it so WWW server vendors supply examples.
- ◆ The examples have security holes in them. Some CGI programmers haven't checked their code.

10

Most WWW server code contains examples of CGI-BIN scripts in the cgi-bin subdirectory. These examples are for illustrative purposes and were not written with any security in mind. Hackers have discovered that they can subvert these programs and cause them to run other programs. You should remove all of these examples from your production www server. There's no need for them to be on the system.

As always, you should always check to make sure your www server code is updated on a regular basis with the latest security patches.




The Second Item – CGI Scripts

- ◆ All Web servers could be affected by this “feature”.
- ◆ **The Danger**
 - Your WWW pages could be changed a la DOJ, CIA, FBI, Valujet.
 - Your WWW server could be used to attack other sites
- ◆ **A Solution**
 - Remove unsafe CGI scripts from the WWW server

11

www.2600.com lists www sites that have been compromised by hackers. It also shows what the modified www page looks like to the visitor. Take a look at a couple of them and ask yourself, “can my company afford this happening to it?”.

Your www pages may be intact, but the hackers may use your system to attack other sites. Gee, does this sound familiar?




Item #3: Remote Procedure Calls (RPC)

- ◆ RPC allows a computer to run a program on another computer.
- ◆ It's used by computers that share files between them.
- ◆ Many client – server systems depend on the use of RPC calls.
- ◆ UNIX systems (Solaris, AIX, HP-UX, Linux, Tru64, Irix) were primarily affected but any computer that uses the RPC subsystem is vulnerable

12

RPC are the foundation of most client/server programs. The buffer overflow attack is one way hackers can force the RPC subsystem to run a program on the victim system. This programs typically installs a backdoor into the system which the attackers use later to log into the system.




Item #3: Remote Procedure Calls (RPC)

- ◆ **The Danger:**
 - Older versions of RPC have security weaknesses that allow hackers to gain full control of your computer(s).
- ◆ **A Solution**
 - Disable the RPC services if you don't use them
 - Install the latest vendor patches

13

This should sound like a broken record ☹ but once again, the hacker can gain control of your system. The solutions are fairly simple and reasonable. If you don't use the RPC service, disable it. Practically speaking, this isn't a viable solution because just about every client-server program in existence uses RPC to transfer data. So, we go back to our tried and true solution---installing vendor maintenance and security patches.




Item #4: Microsoft Internet Information Server (IIS)

- ◆ Windows NT and Windows 2000 Web servers use IIS to support web services.
- ◆ IIS has a component called Remote Data Services (RDS) that could allow a hacker to run remote commands with administrator privileges.

14

IIS is the web server software found on most www sites deployed on Window NT and 2000 systems. Some of IIS's components are vulnerable to a buffer overflow type of attack which lets the hacker gain full control of the system. Since the hacker can run remote commands on a compromised server, you can imagine the types of abuse that can happen. Obvious things include modifying the www page(s), disabling the server, and launching an attack on a site. More subtle things include adding userids on the server, modifying Active Directory components and installing keystroke recorders on the server system.




Item #4: Microsoft Internet Information Server (IIS)

- ◆ **The Danger:**
 - A hacker can run commands on another system without having to access it directly.
- ◆ **A Solution:**
 - Read the Microsoft technical bulletins that describe how to fix the problem

15

.HTR file exploits are thought to be as common as RDS exploits. As always, proper vendor patch maintenance, monitoring of full disclosure sites such as www.securityfocus.com and vendor security warning information provides the best method of correcting this flaw.



Item #5: Sendmail Weakness


- ◆ Sendmail is one of the original Internet email programs.
- ◆ It was a graduate programming project that was never designed to work in a “production” environment.
- ◆ It became the defacto standard.
- ◆ Pre-version 8.10 had security problems
 - Some vendors still ship Sendmail v5.65!
- ◆ Most vendors shipped their systems with these older versions.

16

Sendmail is the master email program for a majority of the mail servers on the Internet. It is the program that actually processes and sends your email. It is not the front end that you see when you invoke your email program (Eudora, Exchange, pine, elm, exmh).

Sendmail has been constantly upgraded to correct bugs and add features. In the Early 90's, older versions of sendmail were vulnerable to a variety of exploits, the most common being our old friend, the buffer overflow.

Since sendmail runs with root privilege, the consequences of it running an unauthorized program can be quite severe. Some vendors grabbed a version of sendmail when they were developing their own product and then failed to upgrade it in a timely fashion.




Item #5: Sendmail Weakness

- ◆ The 1988 Internet Worm exploited a problem in sendmail. There are a lot of systems that still run that version of sendmail. Why? It works!
- ◆ **The Danger:**
 - Hackers can run commands on your systems without ever logging into your system. Hackers can take over your machine.
- ◆ **A Solution:**
 - Update to the latest version of sendmail

17

Yes, some vendors still ship Sendmail v5.65 which contains more holes than a screen door on a submarine. Most vendors are shipping their product with later versions but it is prudent to get the latest version of sendmail (currently v8.12) and install it on your server systems. The sendmail installation process has been refined considerably over the past decade and it is quite easy to build sendmail installation kits that can be used on your systems.




Item #6: sadmin and mountd

- ◆ Sadmin is used by Solaris applications to run distributed sysadmin operations. It executes the request on the server from a client program. Sounds like RPC? It is.
- ◆ Mountd controls file sharing across the network using NFS. This is the program that “attaches” a remote disk to your computer.

18

Sadmin is specific to Sun Solaris systems. It allows a sysadmin to remotely administer systems on a network. Lab sysadmins may use this tool to help them manage their systems remotely from a single system. It provides the way to let the sysadmin use the nice administration GUI's over the network. The Network File Sharing (NFS) system is the mechanism that allows users to access directories remotely. The mountd program is the “driver” for mounting remote filesystems on UNIX hosts. Early versions of sadmin and mountd are vulnerable to buffer overflow attacks. A successful buffer overflow attack on sadmin or mountd will give the hacker root access on the machine.




Item #6: sadmind and mountd

- ◆ **The Danger:**
 - Hackers can cause these programs to give them access to root. They can take over your machine.
 - This was one of the primary ways hackers used to set up the systems used in the recent DDOS attacks against Yahoo, CNN and other sites.
- ◆ **A Solution:**
 - Install the latest vendor patches for sadmind and mountd.

19

This page intentionally left blank.



Item #7: Global File Sharing


- ◆ You can share files between computers using tools like Network Neighborhood (Windows), AppleShare(Macintosh) or NFS(UNIX).
- ◆ By default, the access is *read-write*.
- ◆ Anyone on the same network could access your files. In the old days, the network was small but now the network is the Internet so anyone anywhere in the world could access your files if you let them.
- ◆ The problem is that you don't always know that you're letting them.

20

More and more computer systems are being connected to the Internet by cable modems, ADSL or other direct connect methods. This means that home systems are now vulnerable to attacks.

One of the simplest methods of gaining information about a victim system is through a file sharing misconfiguration. Network neighborhood really MEANS the network and sometimes, people don't realize the scope of the neighborhood.

Disclosure of personal information is the biggest danger in this case. For example, Windows users may use Microsoft's MSMoney program to manage their personal finances. If the file sharing access controls are set incorrectly, it is possible for someone else on the network to simply connect to the system and copy the MSMoney files to their machine.




Item #7: Global File Sharing

- ◆ This is a real danger to homes that have direct connect modems.
- ◆ **The Danger:**
 - People can get access to your personal data, for example, your checking account data (if you use MSMoney), your email, etc.
- ◆ **A Solution:**
 - Make sure you know what you're sharing.
 - Make sure you know who's sharing the data with you.

21

The basic rule is simple. If you don't use the service, don't enable it. Turn off file sharing on your computer especially if you're using a home computer system. If you must use file sharing, make sure you restrict access only to those people you know. Remember that anyone accessing your files who lets anyone on the net access THEIR files may put your information at risk. This could only happen if the person accessing your files copies them to their system which in turn allows someone else to access them.




Item #8: User Accounts with No Passwords

- ◆ Some systems come with demo or guest accounts with no passwords or well known passwords.
- ◆ The initial/default password for VMS system manager account, SYSTEM was MANAGER. The initial password for the Field Service account, FIELD, was SERVICE.
- ◆ People forgot to change these passwords.
- ◆ The first thing hackers do is check to see if the defaults passwords were changed. Why waste a lot of effort if the door is unlocked?

22

You're always told to make sure you have secure passwords for your manager or administrator account. What do you do when the system is installed for the first time? What is the administrator password? In the old days, vendors would set up a default password for the system. They assumed that you would change the password before the system went into production. Well, some people did just that but others didn't for reasons ranging from laziness to "I thought that password was set up for me". One of the first things hacker try is the list of default passwords for the admin or manager accounts. Some of the well-known ones are listed in the above slide. Remember, the first goal of the hacker is to gain access to the system, then they run a particular exploit against the system to gain administrator status. Why go through all that effort if the door is left open via a default password?




Item #8: User Accounts with No Passwords

- ◆ **The Danger:**
 - Someone can get complete control of your system.
 - Someone can get access to your system via a general accounts and then run exploit tools on your systems to get full control of your system.
- ◆ **A Solution:**
 - Change your root, administrator passwords before the systems goes into production.
 - Run a password checking program to discover who has weak passwords on your system. Do it before the hackers do!

23

You should always check your systems for user accounts that have no passwords assigned to them. Always change your root/admin passwords from the defaults supplied by the vendor.




Item #9: IMAP, POP Vulnerabilities

- ◆ IMAP and POP are two common email protocols that provide additional features to email users.
- ◆ They allow users to access their email accounts from anywhere on the Internet.
- ◆ Firewalls usually allow email using these services to pass through the firewall.
- ◆ Quality control of the software is inconsistent most of the time.

24

IMAP and POP (Post Office Protocol) are 2 email mechanisms that are commonly used by a lot of vendors. Eudora and SIMS are 2 examples of mail programs that use this protocol. Once again, there may be problems in the server code that handles email handled in these protocols.




Item#9: IMAP, POP Vulnerabilities

- ◆ **The Danger:**
 - Hackers can gain access to your internal network if they can subvert IMAP or POP mail server systems.
 - If successful, they gain complete control of your system.
- ◆ **A Solution:**
 - Make sure you've installed the latest patches.
 - Run the services on your mail servers only.

25

Hackers may be able to bypass your firewalls through the mail servers on your systems. This gives them access to your internal systems. Their target may be the mail server itself.




Item #10: SNMP Vulnerabilities

- ◆ Simple Network Management Protocol (SNMP) is used by network managers to monitor the status, performance and availability of the network.
- ◆ The Net Mgrs can remotely manage their routers, printers, systems using SNMP.
- ◆ SNMP has very weak authentication. Its default “password” is “private”.
- ◆ Everyone knows this.

26

The Simple Network Management Protocol is used by your network administrators and technicians to monitor the performance of your company network. It provides them with a way to map, identify and send commands to the individual components of your network. When you use the telephone to make a call, you really don't know how many pieces of equipment handle your call. Well, the same thing happens with the network. There are machines called router, bridges, hubs, switch boxes, all of which enable a physical connection to be made between two systems trying to make a connection. All of these components can be monitored via SNMP.

Well, how do you prevent someone from infiltrating the control structure of your network? The good news is that SNMP nodes are password protected. SNMP calls passwords “community strings”. The bad news is that these passwords are rarely set from the default password (remember Item 8?) and the default password is “private”.




Item #10: SNMP Vulnerabilities

- ◆ **The Danger:**
 - Hackers can gain control of network devices such as routers. They could shut them down.
 - They can map your network w/o your knowledge.
- ◆ **A Solution:**
 - Pick strong community strings (passwords) for your SNMP devices.
 - Make the MIBs read only.

27

By now, you should be able to guess the danger of a hacker knowing the SNMP password (community string). Yep, they can gain control of your network. Note that your data is relatively safe, it's just the traffic flow of your network that's in jeopardy. Think of what would happen if someone took over control of the traffic lights in a city.

As always, make sure your network group has picked strong password (community strings) for ALL of the SNMP capable devices on your network.




Summary

- ◆ Most of the successful system and network attacks exploit a small set of vulnerabilities.
- ◆ The Top 10 list briefly describes this set of vulnerabilities and gives you references to learning more about them.
- ◆ More importantly, it gives you some suggested fixes for the problem.
- ◆ Our individual security depends on our mutual security.

28

Most of the successful attacks on Internet hosts have exploited a small number of security vulnerabilities. The Top 10 list describes those vulnerabilities and is designed to give you a starting place for evaluating your system and network security. There are literally thousands of vulnerabilities out there and this list hopefully will help you spend your limited security budget on the most effective tools.



Summary

- ◆ You won't eliminate all of your exposure by closing these 10 holes. *Constant vigilance and awareness is the best defense.*
- ◆ The consequences of failure could drive your company out of business.
- ◆ There'll be another top 10 items to inspect in the future but at least we got rid of these items.

29

Remember: ***closing the Top 10 holes will not guarantee your system or network is safe from hackers!***

It will help close the most common holes that exist today. Constant vigilance is the rule of the day. Think of the Top 10 list as an antiviral tool. It will close KNOWN holes but is vulnerable to NEW holes. Sometime later, there'll be another version of the Top 10 list listing these newer vulnerabilities.



References

- ◆ The complete Top 10 document can be found at <http://www.sans.org/topten.htm>
- ◆ Some WWW sites to visit:
 - www.sans.org
 - www.cert.org
 - www.nipc.gov
 - www.securityfocus.com
 - www.rootshell.com
 - security.vt.edu
 - www.cornell.edu/CPL

30

This page intentionally left blank.



Original author: Randy Marchany, Virginia Tech
v1.1 – edited by S. Northcutt, December 2000