ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

Computer Attacks: What They Are and How to Defend Against Them

Introduction

Using malicious programs like WinNuke, Papa Smurf, and Teardrop, intruders invade our privacy and undermine the integrity of our computers. In the 1999 Computer Security Institute/FBI computer crime survey, fifty-seven percent of organizations cite their Internet connection as a "frequent point of attack." Thirty percent reported that they had found actual intrusions into their networks and 26 percent reported theft of proprietary information. The incident handling entity for the civilian government, FedCIRC, reported that 130,000 government sites totaling 1,100,000 hosts were subject to attacks in 1998. Computer crime is substantial. It is clear that we must increase our efforts to secure our systems and mitigate crime in the relatively new medium of cyberspace.

In order to prevent attacks in cyberspace, systems administrators need a high-level understanding of the methods attackers use to penetrate computers. You cannot effectively fight a war without some knowledge of the weapons of your enemy. The Information Technology Laboratory, National Institute of Standards and Technology, researches the tricks of intruders and educates the public on how to stop them. This bulletin:

- Presents an overview of hacker tools that penetrate computers;
- Classifies the various attacks that attackers use against networks;
- Statistically explores what kinds of computer attacks are being publicly published on the Internet;
- Lists the most popular attacks on the Internet today; and
- Discusses security solutions that can prevent the majority of publicly available computer attacks.

Overview of Attacker Tools

Vast resources are available on the Internet that enable intruders to penetrate computer networks. Detailed software vulnerability information is publicly discussed on newsgroups. Attacking tutorials are available that describe how to write automated programs that penetrate computers by taking advantage of these vulnerabilities. Thousands of automated software tools have been written that enable anyone to launch computer attacks. Computer attacks are no longer found on obscure pirate bulletin boards but rather on publicly available commercial Web sites whose sole purpose is to serve up this information.

These computer attack programs are freely available to anyone on the Internet. Besides being available, these attacks are becoming easier to use. A few years ago, one had to have Unix to run an attack and had to know how to compile source code. Today, attacks with user-friendly graphical user interfaces (GUIs) that run on Windows hosts are available. Attack scripts are easy to use and dangerous. It is vital that systems administrators understand the danger these attacks pose and how to protect their networks against them.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since February 1998

Classification of Computer Attacks

When we say "computer attack," we mean programs run by people to gain unauthorized control over a computer. These attacks take a variety of forms but generally fall in the following categories:

1. **Remote Penetration**: Programs that go out on the Internet (or network) and gain unauthorized control of a computer
2. **Local Penetration**: Programs that gain unauthorized access to the computer on which they are run
3. **Remote Denial of Service**: Programs that go out on the Internet (or network) and shut down another computer or a service provided by that computer
4. **Local Denial of Service**: Programs that shut down the computer on which they are run
5. **Network Scanners**: Programs that map out a network to figure out which computers and services are available to be exploited
6. **Vulnerability Scanners**: Programs that scour the Internet looking for computers vulnerable to a particular type of attack
7. **Password Crackers**: Programs that discover easy-to-guess passwords in encrypted password files. Computers can now guess passwords so quickly that many seemingly complex passwords can be guessed.
8. **Sniffers**: Programs that listen to network traffic. Often these programs have features to automatically extract usernames, passwords, or credit card information.

Statistical Sampling of Publicly Available Computer Attacks

In 1998, NIST categorized and analyzed 237 computer attacks that were published on the Internet out of an estimated 400 published attacks. This sample yielded the following statistics:

Statistic:	29% of attacks can launch from Windows hosts
Lesson:	One does not need to understand Unix to be dangerous anymore. We are in an era of “point and click” attacks.
Statistic:	20% of attacks are able to remotely penetrate network elements (e.g., routers, switches, hosts, printers, and firewalls)
Lesson:	Attacks that give remote users access to hosts are not rare.
Statistic:	3% of the attacks enable Web sites to attack those who visited the site
Lesson:	Surfing the Web is not a risk-free activity.
Statistic:	4% of attacks scan the Internet for vulnerable hosts
Lesson:	Automated scanning attack tools, which find easily compromised hosts, abound. System administrators, with management concurrence or with professional assistance, should scan their own systems regularly before someone else does.
Statistic:	5% of attacks are effective against routers and firewalls
Lesson:	The Internet infrastructure components themselves are vulnerable to attack. (To the computer industry's credit, most attacks were denial of service and scanning and only a few were penetration attacks.)

The Most Popular Attacks on the Internet

In March 1999, the most popular attacks (or vulnerable applications) found by NIST were Sendmail, ICQ, Smurf, Teardrop, IMAP, Back Orifice, Netbus, WinNuke, and Nmap. These are discussed below.

1. **Sendmail**: Sendmail is an extremely old program that has had vulnerabilities throughout its history. Sendmail is proof that complex software is rarely completely patched because developers constantly add new features that introduce new vulnerabilities. Recent attacks against sendmail fell into the categories of remote penetration, local penetration, and remote denial of service.
2. **ICQ**: ICQ is a sophisticated chat program that stands for "I-Seek-You." It is currently owned by America Online and used by over 26 million users. In the past year, several ICQ attacks were developed that allowed one to impersonate other people and decrypt "encrypted" traffic. An attacker would use these attacks by going to a chat room and finding two people that are friends. The attacker then pretends to be someone’s friend and sends them a Trojan horse (malicious code embedded into a legitimate program) via ICQ.
3. **Smurf**: Smurf uses a network that accepts broadcast ping packets to flood the target with ping reply packets. Think of smurf as an

amplifier allowing an attacker to anonymously flood a target with a huge amount of data.

4. **Teardrop**: Teardrop freezes vulnerable Windows 95 and Linux hosts by exploiting a bug in the fragmented packet re-assembly routines.

5. **IMAP**: The Internet Message Access Protocol (IMAP) allows users to download their e-mail from a server. Last year, IMAP server software was released with a vulnerability that allows a remote attacker to gain complete control over the machine. This vulnerability is extremely important because a large number of mail servers use the vulnerable IMAP software.

6. **Back Orifice**: Back Orifice is a Trojan horse that allows a user to control remotely a Windows 95/98 host with an easy-to-use GUI.

7. **Netbus**: Netbus is similar to Back Orifice but it works against Windows NT as well as Windows 95/98.

8. **WinNuke**: WinNuke freezes a Windows 95 host by sending it out-of-band TCP data.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

9. **Nmap**: Nmap is a sophisticated network-scanning tool. Among other features, nmap can scan using a variety of protocols, operate in stealth mode, and automatically identify remote operating systems.

How to Prevent the Majority of Computer Attacks

Protecting one's networks from computer attacks is an ongoing and non-trivial task; however, some simple security measures will stop the majority of network penetration attempts. For example, a well-configured firewall and an installed base of virus checkers will stop most computer attacks. Here, we present a list of 14 different security measures that, if implemented, will help secure a network.

1. ***Patching***
   Companies often release software patches in order to fix coding errors. Unfixed, these errors often allow an attacker to penetrate a computer system. Systems administrators should protect their most important systems by constantly applying the most recent patches. However, it is difficult to patch all hosts in a network because patches are released at a very fast pace. Focus on patching the most important hosts and then implement the other security solutions mentioned below. Patches usually must be obtained from software vendors.

2. ***Virus Detection***
   Virus-checking programs are indispensable to any network security solution. Virus checkers monitor computers and look for malicious code. One problem with virus checkers is that one must install them on all computers for maximum effectiveness. It is time-consuming to install the software and requires updating monthly for maximum effectiveness. Users can be trained to perform these updates but they can not be relied upon. In addition to the normal virus checking on each computer, we recommend that organizations scan e-mail attachments at the e-mail server. This way, the majority of viruses are stopped before ever reaching the users.

3. ***Firewalls***
   Firewalls are the single most important security solution for protecting one's network. Firewalls police the network traffic that enters and leaves a network. The firewall may outright disallow some traffic or may perform some sort of verification on other traffic. A well-configured firewall will stop the majority of publicly available computer attacks.

4. ***Password Crackers***
   Hackers often use little-known vulnerabilities in computers to steal encrypted password files. They then use password-cracking programs that can discover weak passwords within encrypted password files. Once a weak password is discovered, the attacker can enter the computer as a normal user and use a variety of tricks to gain complete control of your computer and your network. While used by intruders, such programs are invaluable to systems administrators. Systems administrators should run password-cracking programs on their encrypted password files regularly to discover weak passwords.

5. ***Encryption***
   Attackers often break into networks by listening to network traffic at strategic locations and by parsing out clear text usernames and passwords. Thus, remote password-protected connections should be encrypted. This is especially true for remote connections over the Internet and connections to the most critical servers. A variety of commercial

and free products are available to encrypt TCP/IP traffic.

6. ***Vulnerability Scanners***
Vulnerability scanners are programs that scan a network looking for computers that are vulnerable to attacks. The scanners have a large database of vulnerabilities that they use to probe computers in order to determine the vulnerable ones. Both commercial and free vulnerability scanners exist.

7. ***Configuring Hosts for Security***
Computers with newly installed operating systems are often vulnerable to attack. The reason is that an operating system's installation programs generally enable all available networking features. This allows an attacker to explore the many avenues of attack. All unneeded network services should be turned off.

8. ***War Dialing***
Users often bypass a site's network security schemes by allowing their computers to receive incoming telephone calls. The user enables a modem upon leaving work and then is able to dial in from home and use the corporate network. Attackers use war dialing programs to call a large number of telephone numbers looking for those computers allowed to receive telephone calls. Since users set up these computers themselves, they are often insecure and provide attackers a backdoor into the network. Systems administrators should regularly use war dialers to discover these back doors. Both commercial and free war dialers are readily available.

9. ***Security Advisories***
Security advisories are warnings issued by incident response teams and vendors about recently discovered computer vulnerabilities. Advisories usually cover only the most important threats and thus are low-volume and high-utility reading. They describe in general terms the threat and give very specific solutions on how to plug the vulnerability. Excellent security advisories are found from a variety of sources, but the most popular come from the Carnegie Mellon Emergency Response Team at http://www.cert.org.

10. ***Intrusion Detection***
Intrusion detection systems detect computer attacks. They can be used outside of a network's firewall to see what kinds of attacks are being launched at a network. They can be used behind a network's firewall to discover attacks that penetrate the firewall. They can be used within a network to monitor insider attacks. Intrusion detection tools come with many different capabilities and functionality. For a paper on the uses and types of intrusion detection systems, see http://www.icsa.net/services/consortia/intrusion/educational_material.shtml.

11. ***Network Discovery Tools and Port Scanners***
Network discovery tools and port scanners map out networks and identify the services running on each host. Attackers use these tools to find vulnerable hosts and network services. Systems administrators use these tools to monitor what host and network services are connected to their network. Weak or improperly configured services and hosts can be found and patched.

12. ***Incident Response Handling***
Every network, no matter how secure, has some security events (even if just false alarms). Staff must know beforehand how to handle these events. Important points that must be resolved are: when should one call law enforcement, when should one call an emergency response team, when should network connections be severed, and what is the recovery plan if an important server is compromised? CERT provides general incident handling response capabilities for our nation (http://www.cert.org). FedCIRC is the incident response handling service for the civilian federal government (http://www.fedcirc.gov).

13. ***Security Policies***
The strength of a network security scheme is only as strong as the weakest entry point. If different sites within an organization have different security policies, one site can be compromised by the insecurity of another. Organizations should write a security policy defining the level of protection that they expect to be uniformly implemented. The most important aspect of a policy is creating a uniform mandate on what traffic is allowed through the organization's firewalls. The policy should also define how and where security tools (e.g., intrusion detection or vulnerability scanners) should be used in the network. To obtain uniform security, the policy should define secure default configurations for different types of hosts.

14. ***Denial-of-Service Testing (for firewalls and Web servers)***
Denial-of-service (DOS) attacks are very common on the Internet.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Malicious attackers shut down Web sites, reboot computers, or clog up networks with junk packets. DOS attacks can be very serious, especially when the attacker is clever enough to launch an ongoing, untraceable attack. Sites serious about security can launch these same attacks against themselves to determine how much damage can be done. We suggest that only very experienced systems administrators or vulnerability analysis consultants perform this type of analysis.

For More Information

More details on computer attacks can be found in the paper "Understanding the Global Attack Toolkit Using a Database of Dependent Classifiers" at the URL: http://www.itl.nist.gov/div893/staff/mell/pmhome.html

General computer security information:

NIST Computer Security Resource Clearinghouse: http://csrc.nist.gov

Federal Computer Incident Response Capability: http://www.fedcirc.gov

Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu

Carnegie Mellon Emergency Response Team: http://www.cert.org

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300

Address Service Requested