GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Name: Vincent Vono
Version number: 1.2e
Title: A General Overview of Attack Methods

Introduction

The purpose of this paper is to present a general overview of various attack methods which are used by attackers to compromise network security, as well as understanding how some attacks occur, how to prevent them and knowing what solutions can be implemented so they will not succeed. Attack types include information gathering, misadministration, software bugs and denial of service. Types and variations of attacks are numerous, and usually can be grouped into one of the following four categories:

- Information Gathering
- Unauthorized Access
- Disclosure of Information
- Denial of Service

Information Gathering

Information gathering is actually not an attack type, rather a set of actions an attacker may perform to gather data about the computers, services and/or users. It is a set of actions that lead up to an attack.

Social Engineering

One method to gather information or to open security holes is called "Social Engineering", which is as simple as talking to people. The attacker may pretend to be someone that is in a position of trust, attempts to gain a person's confidence, and then to get him/her to violate your security policy. It is more psychology than engineering, as the attacker relies on his conversation skills and self-confidence (sounds like a con-artist, doesn't it?). How can you defend against this type of attack? Unfortunately, this is not easy, but educating your users on a regular basis is a good start. This starts with a sound security policy, indicating to always have your users verify a person's identity and authority, before responding to a situation that may compromise security. We want people to be aware of social engineering, but it can be inefficient to have everyone paranoid.

Dumpster Diving / Shoulder Surfing

There are other methods an attacker may use to gather information to prepare for an attack. One of these methods is called "Dumpster Diving", which is just what it sounds like. Dumpster diving is the art of searching through an organization's trash to find things like company directories, notes with passwords scribbled on them, organizational charts containing the names of your organization's staff (which can be used to impersonate a staff member in a social engineering attempt), network diagrams, etc… anything that will

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

assist to simplify an attack. “Shoulder Surfing” is another method, referring to looking over someone’s shoulder as they are keying in their personal credit card number, telephone number, passwords, etc. Shoulder surfing is most effective at busy locations, such as an airport or a train station. Again, user education is the means to combat these types of information gathering, to block the leaking of information before it is too late.

Sniffing

“Sniffing”, named after the commercial product from Network Associates, Inc., is the process of reading network traffic via a protocol analyzer. This is a viable information-gathering tool, since many protocols do not encrypt sensitive information. If an attacker can compromise a host anywhere on the network, he can either run a readily available protocol analyzer from that host, or download one of their own. Taking steps to block physical access to you network and hosts, as well as hardening the hosts on your network to avoid a compromise is a good solution.

Basic Services

Another means for information gathering is the use of “Basic Services”, such as FINGER, NETSTAT, and the SMTP primitives VRFY and EXPN. These types of services are still widely enabled and can be used by an attacker to find out information about users or see if particular accounts exist. Disable these services if they are not needed.

Scanning and Version Information

“Scanning” refers to the process of attempting to connect to a range of port numbers or IP addresses to see what services or computers exist and if they are turned on. It is probably the most widely used method by attackers to find out if what they are scanning is going to be their next potential victim. Scanning tools are automated, and there are numerous flavors of these tools available to aid an attacker. Another method of scanning, called “War Dialing”, is the scanning of phone numbers in an attempt to find ones with modems on them in the hopes that the attacker can break into the computer via the attached modem. Modems are often setup in an organization without the knowledge or approval of an organization’s IT or security group. These back doors to an organization’s infrastructure are usually poorly secured (if secured at all) which makes the attacker’s job easier to gather information or break into a system. The best solution for these types is to limit the exposure by blocking or turning off any IP addresses, port numbers, or modems that are not necessary. Scanning and war dialing are also useful means for the security or network administrators, to help find unauthorized hosts or services before the attackers do. Also, “Version Information” is something an attacker will always look for, with the hopes that it shows an unpatched system that is vulnerable to a security hole. It helps to turn this off, if possible. In any case and very important, always ensure the latest and greatest security patches from your vendor have been applied.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Misadministration

Hackers will also be on the lookout to exploit systems that have trust relationships that may have been misadministered. Trust relationships can range from basic user accounts allowing people to access computer resources; to services of other networked computers which users or computers are allowed to have access to. "Individual User Accounts" are the most basic trust relationship. Accounts come with passwords, which users tend to use passwords that are easy to remember. On the other hand, if users are forced to use account passwords that are difficult to remember, most likely they are writing them down or recording them somewhere, which is considered to be more insecure. Passwords are also susceptible to being sniffed by an attacker; maybe a reusable password being viewed in plaintext as it passes over the network. There are vulnerabilities for encrypted passwords an attacker may exploit as well. If an attacker can get a copy of the file storing encrypted passwords, there are readily available password cracking tools downloadable from the Internet for free that will guess passwords using brute force. Attackers have plenty of time on their hands to crack passwords. These tools will encrypt dictionary words using various permutations, then compare to the encrypted values of the stolen password file. Once one is matched, the attacker has the access. Ensure you have a very strong, enforceable user account/password policy as well as the use of strong authentication using one time passwords whenever possible. Also, implementing devices such as token cards that use an encrypted scheme for passwords will make it virtually impossible for an attacker to guess or reuse a password.

"Berkeley r Commands". These commands allow users log onto, run commands or shells, and copy files between networked computers without the need to separately authenticate on each computer. These trust relationships are created using either of two files on the trusting computer, hosts.equiv or .rhosts, which is based on user account names and the IP addresses of the computers included in the trust model. If these utilities are needed, they should be administered carefully, granting minimal privileges. Also, unless you trust your users to be well educated, consider not allowing the users to administer their own trust or even better, turn the service off completely by disabling the daemons associated with the service, like rlogind and rshd.

Exploiting Non-Authenticated Services

There are a number of network services that do not use any authentication. These services can be easily spoofed, or can be used to access or modify information on a victim's host. TFTP (Trivial File Transfer Protocol) does not use logins or passwords, and relies only on file system access permissions. It can be used by an attacker to obtain files, such as password files for later decoding, or other sensitive information. SMTP (Simple Mail Transfer Protocol), the standard e-mail protocol, has no mechanisms for positively identifying the sender of an e-mail, making it very easy for an attacker to spoof e-mail. DNS (Domain Name Service) uses a hierarchy of name servers to look up IP addresses for domain names. It can be spoofed by sending unsolicited incorrect responses, causing the end user to be connected to the wrong host. RIP and IGRP are routing protocols used by routers and hosts, which broadcast information of how to route to other networks.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

They have no authentication, so any host or router listening for RIP or IGRP packets could be misdirected to an attacker's network. The attacker could then intercept and/or monitor traffic. The best solution to the vulnerabilities these services cause is to turn off their respective services, or limit their use and access to trusted network environments only. Some services, like SMTP, are quite essential to block so severely. Here, the best solution is to be aware of the vulnerabilities within and not to trust too much, or establish some type of trust mechanism on top of it, such as encryption.

Exploiting Centralized Services

There are some network services which aid in assisting network administrators in managing networked hosts and these services can also be susceptible to vulnerabilities if not properly administered or accessed outside your trusted network. SNMP (Simple Network Management Protocol), which is used to manage network devices and read traffic information, uses a community name as its password. This password is transmitted as clear-text and is usually set to the word public, which makes it very easy for an attacker to guess. NIS (Network Information Service), is used to centrally administer common files on networked hosts, such as /etc/passwd and /etc/hosts. NIS uses a domain name, which is usually similar to the network's DNS domain name, making it relatively easy for an attacker to guess. Remote Registry is used to centrally manage Microsoft hosts. An attacker can access the registry if it is incorrectly administered. These services mentioned above need to be administered securely and isolated to trusted network access only to prevent an attacker from accessing these services from the outside.

Malicious Data

Malicious data is information input to programs that can cause the program to take action that the program would not normally do or cause damage to the host system. Also, new features within programming allow much more action to be taken based on input data. These features can come in the form of macros, auto play features, Java and ActiveX, and postscripts. They add power to applications, such as inputting data automatically into an application or downloading executable data to be run on a client's computer. Unless the applications take a great effort to check input data, these features can be used to unintentionally and possibly unknowingly modify information on a client's host. Programs that accept user input should make no assumptions about the validity of the input or where the input came from. Some examples of invalid input data to programs are extra characters entered into an extended data field, or data entered into a field that should only allow choices from a pre-defined list for that field. Buffer overflows, which are used either to crash a system or possibly gain access to it, are highly technical attacks. They count on variables not being tested or variables that are bound for length. By carefully crafting the bytes of information, an attacker can get a program to run their own code. The code is sent as an input string, which is larger than the buffer's space allocated by the program, and overwrites the next bytes in memory, which often contains the stacker point values. The pointer values tell that part of the program where to go to execute its next instructions. For this type of attack to work, the attacker needs to know

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

how to craft the specific machine language instructions, and know how memory and computer architecture work in detail. The target must be a specific variable in a specific program. An attacker may have the same setup available to experiment on how to get the attack to work. Even if the attacker cannot get their own code to run, they may be able to cause the system to lock up or reboot. Programmers need to test the length of all input variables and test the input data of their programs to avoid buffer overflows.

Spoofing

Basically, spoofing is pretending to be someone or something you are not. User account spoofing is using another person's account name and password without their permission or authority. Sniffing the network or breaking password files aids an attacker in user spoofing. DNS spoofing can be done by sending an unsolicited DNS response to a name server on the victim's network, or by trying to beat a real DNS response back to the same name server. An automated sniffing program can aid to detect queries and then insert a corrupted response. This may be hard to prevent, but also hard to execute. IP address spoofing is dependent on the fact that virtually all routers in networks look at only the destination IP address in an IP header, but rarely look at the source IP address. For this type of attack to work, it cannot depend on getting any reply packets back to the attacking host. IP address spoofing can be easily prevented by filtering on the source IP address at the point the packet enters into your network, assuming an attacker is attempting to spoof one of your internal hosts that is trusted by the victim host.

Denial of Service

DoS (denial of service) attacks cause the loss of access to a resource rather than allow the attacker to gain unauthorized access to the resource. They usually involve overloading a resource such as disk space, network bandwidth, internal tables of memory or input buffers (buffer overflow). The overload causes the host or particular service to become unavailable for legitimate use. This could be blocking access to a resource all the way up to causing a host to crash. There are numerous denial of DoS attacks and the solutions to them are not always easy. Some attacks, such as ICMP based attacks, can be blocked with filters. Others can be as simple as turning the particular service off if it is not needed. But others cannot be easily blocked while still allowing normal use of the service. This is another type of Dos, because if an attacker's potential threat forces you to turn off a service that you want to use, then the attacker has accomplished their goal; making the service unavailable to you.

Summary

There are numerous attack methods concerning network security that continue to grow and change. This paper does not nearly address them all; rather I hope it has been a starting point for some categories and topics to look for. Security is rarely designed upfront within systems and it is very difficult to close every security hole in one's organization, especially large organizations. A comprehensive security policy associated with various procedures is the key to implementation. Ensure users are aware of what is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

expected of them. Ensure your organization has a comprehensive incident handling procedure to handle attacks. And probably most of all, it is very important to keep yourself up to date on network security issues. Knowledge of the attack methods that are old and new is crucial to combat them.

Resources

CERT® Advisory CA-1991-04 Social Engineering
http://www.cert.org/advisories/CA-1991-04.html

Protecting Network Infrastructure at the Protocol Level
Curt Wilson / December 15, 2000
http://www.sans.org/infosecFAQ/threats/protocol_level.htm

Blocking Buffer Overflow Attacks; Network Magazine, Rik Farrow
http://www.networkmagazine.com/article/NMG20000511S0015

Malicious Data and Computer Security, Olin Sebert
http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper048/MALDATA.PDF

Network Security Administration; Global Knowledge Inc.; M9800-001 October 1999

Denial of Service; What is it, how does it happen, and how to protect yourself
http://netsecurity.about.com/compute/netsecurity/library/weekly/aa052501a.htm

Computer Crimes Examples of Network Security Attacks
http://www.leccorder.com/content/seminars/Security-23Apr1999/Slides/

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.