International Journal of Engineering Research ISSN: 2348-4039
& Management Technology
September- 2015 Volume 2, Issue-5
Email: editor@ijermt.org www.ijermt.org

Manet Security: Threats & Precautions

Pawan Ahuja
Research Scholar
Department of Computer Science & Engg.
Sunrise University
Alwar

Sudhir Dawra
Associate Professor
Department of Computer Science & Engg.
Ideal Institute of Technology
Ghaziabad

ABSTRACT:
MANET security is a complicated field, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired", an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them.
MANET security is the process of preventing and detecting unauthorized use of our network. Prevention measures help us to stop unauthorized users (also known as "intruders") from accessing any part of our computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

SIGNIFICANCE OF SECURITY:
It's very important to understand that in security, one simply cannot say ``what's the best firewall?" There are two extremes: absolute security and absolute access. The closest we can get to an absolutely secure machine is one unplugged from the network, power supply, locked in a safe, and thrown at the bottom of the ocean. Unfortunately, it isn't terribly useful in this state. A machine with absolute access is extremely convenient to use: it's simply there, and will do whatever you tell it, without questions, authorization, passwords, or any other mechanism.
Every organization needs to decide for itself where between the two extremes of total security and total access they need to be. A policy needs to articulate this, and then define how that will be enforced with practices and such. Everything that is done in the name of security, then, must enforce that policy uniformly.

KEYWORDS: - MANET Security, Threats, Denial-of-Service, attackers, access, Data Diddling, Data Destruction, Firewalls, Demilitarized Zone, Packet Filtering.

TYPES AND SOURCES OF MANET THREATS:
We have covered enough background information on networking that we can actually get into the security aspects of all of this. First of all, we will get into the types of threats there are against networked computers, and then some things that can be done to protect yourself against various threats.

DENIAL-OF-SERVICE:
DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they are very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.
The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and

telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the web site running there, for example).

Some things that can be done to reduce the risk of being stung by a denial of service attack include

- Not running your visible-to-the-world servers at a level too close to capacity
- Using packet filtering to prevent obviously forged packets from entering into your network address space.
- Keeping up-to-date on security-related patches for your hosts' operating systems.

UNAUTHORIZED ACCESS:

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

EXECUTING COMMANDS ILLICITLY:

It's obviously undesirable for an unknown and untrusted person to be able to execute commands on your server machines. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

CONFIDENTIALITY BREACHES:

We need to examine the threat model: what is it that you're trying to protect yourself against? There is certain information that could be quite damaging if it fell into the hands of a competitor, an enemy, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage.

While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for your computer on their screen, there are those who are more malicious.

DESTRUCTIVE BEHAVIOR:

Among the destructive sorts of break-ins and attacks, there are two major categories.

DATA DIDDLING:

The data diddler is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. An accounting procedure might turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once that problem is discovered, how can any of your numbers from that time period be trusted? How far back do you have to go before you think that your data is safe?

DATA DESTRUCTION:

Some of those perpetrate attacks are simply twisted jerks who like to delete things. In these cases, the impact on your computing capability -- and consequently your business -- can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

FIREWALLS:
The discussion of the Internet and similar networks, connecting an organisation to the Internet provides a two-way flow of traffic. This is clearly undesirable in many organisations, as proprietary information is often displayed freely within a corporate intranet.
In order to provide some level of separation between an organisation's intranet and the Internet, firewalls have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

BASTION HOST:
A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other untrusted network). Typically, these are hosts running a flavor of the Unix operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and in many cases, completely removed, in order to improve the security of the machine.

ROUTER:
A special purpose computer for connecting MANETs together Routers also handle certain functions, such as routing, or managing the traffic on the networks they connect.

ACCESS CONTROL LIST (ACL):
Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service port, and so on. These can be employed to limit the sorts of packets that are allowed to come in and go out of a given MANET.

DEMILITARIZED ZONE (DMZ):
The DMZ is a critical part of a firewall: it is a network that is neither part of the untrusted network, nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous: someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

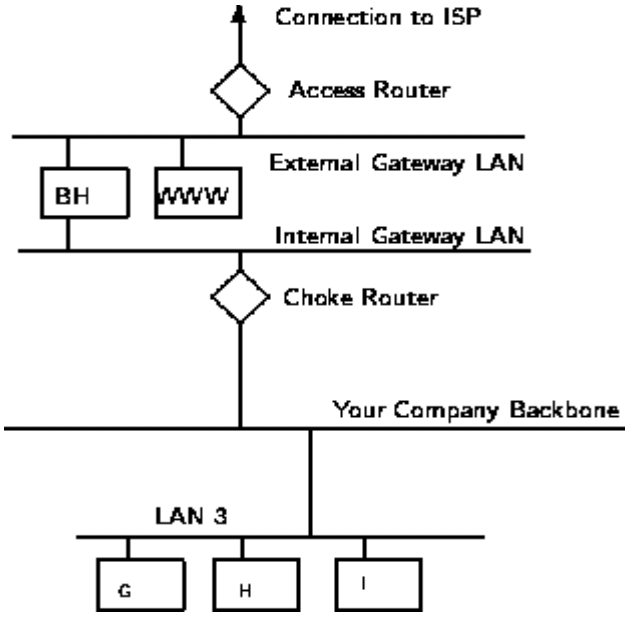
PROXY:
This is the process of having one host act in behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a proxy server, and host on the intranet might be configured to be proxy clients. In this situation, when a host on the intranet wishes to fetch the <http://www.jmi.nic.in/> web page, for example, the browser will make a connection to the proxy server, and request the given URL. The proxy server will fetch the document, and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

TYPES OF FIREWALLS:
There are three basic types of firewalls, and we'll consider each of them.

APPLICATION GATEWAYS:

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server. This software runs at the Application Layer of our old friend the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy, and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic.

A sample application gateway



PACKET FILTERING:

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

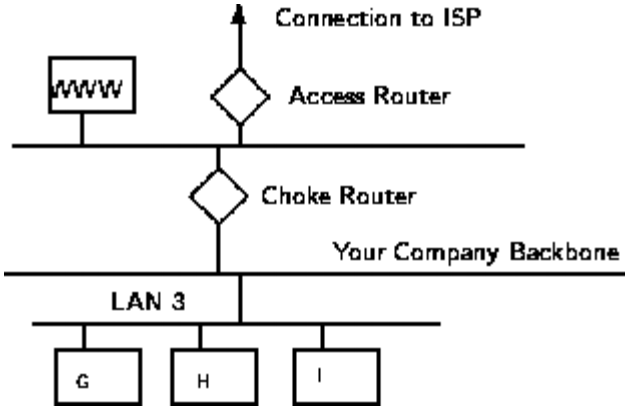
There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins.

There are problems with this method, though. TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, we have to use layers of packet filters in order to localize the traffic. We can't get all the way down to the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal MANET.

HYBRID SYSTEMS:

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

A sample packet filtering gateway



In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed.
Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network.

TYPES OF ATTACKS:

TROJAN HORSE PROGRAMS:

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

BACK DOOR AND REMOTE ADMINISTRATION PROGRAMS:

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer.

DENIAL OF SERVICE:

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack. It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

BEING AN INTERMEDIARY FOR ANOTHER ATTACK:

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system.

UNPROTECTED WINDOWS SHARES:

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet

is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking.

MOBILE CODE (JAVA/JAVASCRIPT/ACTIVEX):

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser.

Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

CROSS-SITE SCRIPTING:

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

You can potentially expose your web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to

using interactive forms on an untrustworthy site viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

EMAIL SPOOFING:

Email “spoofing” is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering ploys. Examples of the latter include email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information. Also, most legitimate service providers would never ask you to send them any password information via email. If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately.

EMAIL BORNE VIRUSES:

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs. Many recent viruses use these social engineering techniques to spread. Never run a program unless you know it to be authored by a person or company that you trust.

HIDDEN FILE EXTENSIONS:

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows. Multiple email-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm which contained an email

attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

CHAT CLIENTS:

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type. Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat client's ability to execute downloaded files.

PACKET SNIFFING:

A packet sniffer is a program that captures data from information packets as they travel over the MANET. That data may include user names, passwords, and proprietary information that travels over the MANET in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access.

CONCLUSIONS:

Security is a very difficult topic. Everyone has a different idea of what ``security" is, and what levels of risk are acceptable. The key for building a secure MANET is to define what security means to your organization. Once that has been defined, everything that goes on with the MANET can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know why what's been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.

REFERENCES:

1. R. Oppliger, Internet and Intranet Security, Artech House, 1998.
2. C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Low Price Edition, Pearson Education, 2007, pp. 521.
3. Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity, September 2006.
4. Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, 2:54-59, 2009.
5. Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.
6. Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis, " Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Mobimedia'09, September 7-9, 2009, London, UK.