IMPLEMENTING DIFFERENT TYPES OF ATTACKS IN NETWORK AND THEIR MITIGATION

Jinia Bhowmik, Prem Lal Daryanani, Sreejon N. Mazumdar, Prof. Somayaji Siva Rama Krishnan
MCA, School of Information Technology & Engineering,
VIT University, Vellore, TamilNadu - 632014, India.
Email: jinia.bhowmik2015@vit.ac.in

Received on 25-10-2016
Accepted on 02-11-2016

Abstract

Background and Objective: With the unparalleled growth in the Internet, network security has become a vital part in maintaining the security of information and the computer as a whole. Materials and Methods: In order to come up with method that make networks more secure, it is important to learn about the vulnerabilities that could be present in a computer network and then have an understanding of the typical attacks that have been carried out in such networks. Results: This paper outlines the classical network attacks that have exploited the typical vulnerabilities of computer networks in the past as well as various defence mechanism against them. Conclusion: This paper will expose the readers to the different network security controls including the network protocols, standards and software/hardware tools that have been adopted in modern day computer networks.

Keywords: Network attacks, Wireshark, LOIC, Burp Suite, Security.

1. Introduction

Network security is an issue that grows in magnitude on a daily basis. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. Network security revolves around the authorization of credentials in order to grant access to data in a network, which is controlled by a network administrator. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. [4] Availability. To secure the information and the entire network system, one specific methodology is required which can be capable of providing the complete security solutions. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. As far as forecasting the emergence of new trends in network security goes, it can be seen that some trends are based on old ideas such as biometric scanning while others are completely new.
2. Materials and Methods

- Types of Basic Attacks

1. Internal Attacks: In an internal attack, the attacker wants to gain access to, and participate in, the network in order to disrupt the network functionality internally. Attackers can join networks by using a fake node for accessing network resources. It has four types:

   1.1. **Dropping Attacks**: A dropping node present in a network behaves like an active node in order to trick the system into transferring through it. Dropping attacks can destroy end-to-end communications between nodes.

   1.2. **Modification Attacks**: Sinkhole attacks are a form of modification attacks, where the malicious node presents itself as a node with the shortest path to the destination. In this way malicious node can access rights to important routing information.

   1.3. **Fabrication Attacks**: Attacker in fabrication attack provides new fake messages in network between nodes to disrupt the routing process.

   1.4. **Timing Attacks**: In this type of attacks, the attacker studies the system and how long it takes for the system to respond to certain situations to discover the vulnerabilities of the system.

2. External Attacks: The attacker aims to cause congestion, initiates fake routing information for destination nodes or disturb nodes from providing services.

   2.1. **Active attack**: It is an attack where attacker can modify data packets, injects the packets, drop the packets thus information can be change in messages.

   2.2. **Passive attacks**: Here the attacker snoops data over the network without changing it. Passive attack target the confidentiality attribute of network and done for recognize the communication pattern between nodes.

Table 1: Types of Network Attacks.
<table>
<thead>
<tr>
<th></th>
<th>Attack Type</th>
<th>Description</th>
<th>Example/Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Active Attack</td>
<td>Active attacks are the most dangerous in natures. In this attack an adversary does not wait for any sensitive or authentication information. He actively tries to break or bypass the secured systems.</td>
<td>It results in disclosing sensitive information, modification of data or complete data lost.</td>
</tr>
<tr>
<td>4</td>
<td>Distributed Attack</td>
<td>In this attack an adversary hides malicious code in trusted software. Later this software is distributed to many other users through the internet without their knowledge.</td>
<td>Pirated software is heavily used for this purpose.</td>
</tr>
<tr>
<td>5</td>
<td>Insider Attack</td>
<td>More than 70% attacks are insider. Insider attacks are divided in two categories: intentionally and accidentally.</td>
<td>Insiders can affect availability by overloading the system’s processing or storage capacity, or by causing the system to crash. They exploit OS bugs to cause the system to crash. The actions are undetected because audit trails are inadequate or ignored.</td>
</tr>
<tr>
<td>6</td>
<td>Phishing Attack</td>
<td>In this attack an adversary creates fake email address or website which looks like a reputed mail address or popular site. Later attacker sends email using their name. These emails contain convincing message, some time with a link that leads to a fake site. This fake site looks exactly same as original site.</td>
<td>Without knowing the truth user tries to log on with their account information, hacker records this authentication information and uses it on real site.</td>
</tr>
<tr>
<td>7</td>
<td>Hijack attack</td>
<td>This attack usually takes place between running sessions. Hacker joins a running session and silent disconnects other party. Then he starts communicating with active parties by using the identity of disconnected party.</td>
<td>Compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.</td>
</tr>
<tr>
<td>8</td>
<td>Spoof attack</td>
<td>In this kind of attack an adversary changes the sources address of packet so receiver assumes that packet comes from someone else.</td>
<td>Bypass the firewall rules.</td>
</tr>
<tr>
<td>No.</td>
<td>Malicious Software Type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9.</td>
<td>Buffer overflow attack</td>
<td>In this attack an adversary sends more data to an application than its buffer size.</td>
<td>It results in failure of service. This attack is usually used to halt a service or server.</td>
</tr>
<tr>
<td>10.</td>
<td>Password attack</td>
<td>Adversary tries to login with guessed password.</td>
<td>Discloses sensitive information, modification of data or complete data lost.</td>
</tr>
<tr>
<td>11.</td>
<td>Packet capturing attack</td>
<td>This attack is part of passive attack.</td>
<td>Attacker extracts information from these packets. This information can be used to deploy several kinds of other attacks.</td>
</tr>
<tr>
<td>12.</td>
<td>Ping sweep attack</td>
<td>In this attack an attacker pings all possible IP addresses on a subnet to find out which hosts are up. Once he finds an up system, he tries to scan the listening ports.</td>
<td>Once the attacker figures out the services, he can try to exploit the vulnerabilities associated with those.</td>
</tr>
<tr>
<td>13.</td>
<td>DNS Query attack</td>
<td>DNS queries are used to discover information about public server on the internet. DNS server respond with internal information such as Server IP address, Email Server, technical contacts etc.</td>
<td>An adversary can use this information in phishing or ping attack.</td>
</tr>
<tr>
<td>14.</td>
<td>MiTM attacks</td>
<td>In this attack an adversary captures data from middle of transmission and changes it, then send it again to the destination.</td>
<td>Receiving person thinks that this message came from original source.</td>
</tr>
<tr>
<td>15.</td>
<td>Denial of Service Attacks</td>
<td>DoS attack is a series of attacks. In this attack an adversary tries to misuse the legitimate services.</td>
<td>In such a situation target host will be too busy in replying (cf ping) that it will not be able run other services.</td>
</tr>
</tbody>
</table>

**Types of Malicious Software**

Software that is harmful to our system and does not have the right permissions from the user of the system or software that gathers information about a user without their consent. The following is a list of terminology commonly used to describe the various types of malicious software:
Table 2: Types of Malicious Software.

<table>
<thead>
<tr>
<th>Sl No.</th>
<th>Name of the Software</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Spyware</td>
<td>It is a technology that aids in gathering information about a person or organization without their knowledge. Spyware can get in a computer as a software virus or as the result of installing a new program.</td>
</tr>
<tr>
<td>2.</td>
<td>Virus</td>
<td>It is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD.</td>
</tr>
<tr>
<td>3.</td>
<td>Worms</td>
<td>A worm is a self-replicating virus that does not alter files but duplicates itself. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.</td>
</tr>
<tr>
<td>4.</td>
<td>LogicBomb</td>
<td>It is programming code, inserted surreptitiously or intentionally, that is designed to execute (or &quot;explode&quot;) under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. It displays or prints a spurious message, delete or corrupt data, or have other undesirable effects after getting executed.</td>
</tr>
<tr>
<td>5.</td>
<td>Trapdoor</td>
<td>It is a method of gaining access to some part of a system other than by the normal procedure. Hackers who successfully penetrate a system may insert trapdoors to allow them entry at a later date, even if the vulnerability that they originally exploited is closed.</td>
</tr>
<tr>
<td>6.</td>
<td>Trojan (Trojan Horse)</td>
<td>It is a program in which malicious or harmful code is contained inside apparently harmless programming in such a way that it can get control and do its chosen form of damage, such as ruining the certain area on your hard disk.</td>
</tr>
<tr>
<td>7.</td>
<td>RATs (Remote Admin Trojans)</td>
<td>These are a special form of Trojan Horse that allows remote control over a machine. These programs are used to steal passwords and other sensitive information.</td>
</tr>
<tr>
<td>8.</td>
<td>Rootkits</td>
<td>These are a set of software tools used by an intruder to gain and maintain access to a computer system without the user's knowledge. These tools conceal covert running processes, files and system data making them difficult to detect. There are rootkits to penetrate a wide variety of operating systems including Linux, Solaris and versions of Microsoft Windows. A computer with rootkits on it is called a rooted computer.</td>
</tr>
</tbody>
</table>
3. Results

Network Security Tools

Security is an important part of networks and its applications. Even though maintaining the security of networks is a significant requirement in the new upcoming networks, there seems to be a major lack of easily implementable protective techniques. Some Network Security tools are listed below:

1. WireShark or Ethereal
2. Burpsuite
3. Low orbit Ion Canon (LOIC)

I. Wireshark:

- It is the one of the most widely and commonly used network protocol tester, which is abundant in its set of features and is also compatible on most of the platforms such as: Microsoft Windows, Linux, UNIX and Macintosh OS X.
- It is commonly used by network system specialists, network surveillance professionals, network builders, and instructors around the world.
- It is freely available tool which is released under the General Public License version 2 (GNU 2).
- It has been created and supported by a universal party of network security protocol experts, and it is an specimen of a disruptive technology.
- Wireshark was previously known as Ethereal.

Figure 1: List of packets displayed by Wireshark.
1.1. Features:

- Wireshark allows the users to intervene and intercept to capture packets which move throughout the network in a specific interface at a specific time instance.
- The interface option in Wireshark, displays a collective series of interfaces on the current node and it allows the capture for nodes.
- The Options tab gives more polished path for every interface individually.
- The go menu’s contents/options enables the users to explore packets in the ‘capture list’.
- The View menu gives us various apparatus for getting a more easy on the eye appearance of the output i.e., packet-list, time, colors.

1.2. Advantages:

- Works with UNIX platform and Microsoft Windows.
- Captures data present within packets being passed around live from network interface.
- Packets are imported from txt files which contain hex dumps of data from packets.
- Packets are displayed with detailed information pertaining to the protocol.
Captured packet data is saved.

Packets are filtered based on certain grounds.

Based on some specific criteria packets are searched.

Packets of a colorized nature are displayed certain filters that are applied.

Abundant statistical data is created.

1.3. Disadvantages:

Does not work as an intrusion detection system. It doesn’t intimate you if someone on the network commits any strange activity on your network which they are by no means permitted to carry out. Wireshark can only help by guiding you to figure out what is actually happening within your network.

It does not make any modifications to the network and can only make some calculated display of information from it.

It does not forward any packets over the network or perform any activities apart from ‘name resolution’.

II. Burpsuite:

Burpsuite is a tool from the house of Port Swigger whose primary objective is penetration testing.

It has been made available for use in two forms i.e., a free trial version and a professional version for paying customers and for commercial use.

Burp works by means of setting up as a proxy to intercept. This way, it is possible to set-up Burp on any environment as a proxy in order to make logs, intercept packets, display & modify HTTP traffic.

Burp can be configured with any application (e.g. Thunderbird, Skype), it is possible, but the most widely used method is by setting up the proxy on a browser that allows the doing so.

Figure 4: Hacking modem page password(192.168.1.1).
2.1. Features:

- An interception proxy can be used to scrutinize and customize the packet traffic between a browser that is set up in a certain way and an application on the web.
- The Spider application of burp suite is can be used to explore functions, features and performance of an application.
- The Repeater tool can manipulate and send numerous requests as an iteration.
- One other important utility in this tool is the decoder, this may be a small feature but is very important – if a packet contains data encoded to a base64 form for example, it can be highlighted, right clicked, and decoded on the fly.

Figure 5: List of routing settings available in BurpSuite.

2.2 Advantages:

- The key role of Burp is to capture packets of HTTP messages and present them in a format more legible and ordered. This giving a user performing tests a quick overview of the targeted system, all messages and other parameterized packets being passed on.
- Burp’s GUI gives a user full control over every message - dropping, forwarding, repeating, modifying, send later, etc.therefore, with the help of these functionalities present within the Burp Suite, a tester can design and simulate various attack scenarios and carry them out manually.
- The results of the various simulated attacks can be viewed directly on the browser and the tester can derive some information from analyzing this.
III. Low Orbit Ion Canon (LOIC)

3.1. Features:

- It was initially built by Praetox Technologies as an open-source tool to perform stress tests on a web application, allowing web developers to simulate a scenario of heavy stress on their server in order to determine how it performs under heavy traffic.

**Figure 6: Targeting a particular ip address using LOIC.**

3.2. Advantages:

- Support both major platforms i.e., Microsoft Windows and Macintosh OS.

- LOIC is a tool that can be used for flooding, thus generating a huge accumulation of network traffic.

**Figure 7: Flooding a particular ip address using LOIC.**

- Even a naive user equipped with L-O-I-C can carry out a denial-of-service (DoS) attack on a victim site or network admin by gaining their ip address and flooding it with fake packets.

- It has been changed/edited in the public domain through several performance updates, patches and bug fixes and been widely used by hacktivist group ‘Anonymous’ as a DDoS tool.
LOIC does not take precautions to hide the IP address of the user, so any attacks generated by this tool are easy to track.

4. Discussions

Jie Shan et. al. [1] discovered during his research that more than 90% of companies every year have suffered from varying virus damages, and that losses in network security amount to almost $7.6 billion in the United States alone. He proposes online anti-virus measures, and safety tools, firewall technologies, and switches to protect against viruses and hackers respectively. Natarajan Meghanathan et. al. [2] states that the problem behind providing proper network security is the ability to differentiate between authorized and unauthorized hosts, and ensuring that the data is made available to the correct party. It had been noticed that IP Spoofing had been the cause behind many attacks. Hence, the networks and hosts that the users are communicating with need to be authenticated, in addition to the users themselves. He further says that instead of relying on a single security control mechanism for all network threats, one must choose the mechanism based on the specific threats that currently exist for the network. It is more favorable for the control mechanism to have changes made only in one layer of the protocol stack than in all layers.

Siddharth Ghansela et. al. [3] lists some basic security tips to secure a network, such as turning off the ping service, closing unused ports, binding IP to MAC address, and using Intrusion Detection Systems. He reiterates the responsibility of the network administrators in checking and deploying missing security patches in all system connected to the network. Performing regular network checks, denying access to unwanted users, and keeping the system updated is also very important in keeping the system and the network secure.

Kartikey Agarwal and Dr. Sanjay Kumar Dubey et. al. [4] argue that a system may be weak by design, configuration, or implementation, which can render it to a threat. Threats may also be caused due to man made or natural disasters, and some may also be a result of human vulnerabilities. A network admin can many of the threats by closely monitoring the network and applying the necessary measures in a timely manner. Other acts such as configuration management, building firewalls, encryption, implementing techniques to defend against DOS attacks, vulnerability testing, etc. are also ways to protect the system. New methods of protection are also being looked into in order to battle the rise in new and sophisticated attacking strategies.

D. Atkins and R. Austein et. al. [5] bring to attention that even though the DNS Security Extensions (DNSSEC) have been under development for a while, it has never been specifically stated which threats the DNSSEC is supposed to safeguard against. It is known that the DNS is susceptible to threats like packet interception, ID guessing and query
prediction, and DoS, to name a few. After documenting the threats and weighing them against the weaknesses that DNSSEC possesses, one may obtain a measure of the extent to which it is useful in protecting against these threats. CarolinLaztzeet. al. [6] discusses various solutions against attacks like phishing, pharming, and Man in the Middle; solutions such as displaying authenticity certificates or logos on the sites, enforcing different passwords for different accounts, coupling SSL and user authentication, and using trusted devices to facilitate authenticity of the user. She also provides a solution involving the trusted device being able to provide cryptographic functions and store keys in a secure environment, and using a form of two channel authentication to provide protection against the attacks. Dennis Cox and Kip McClanahan et. al. [7] propose a method for blocking DoS and address spoofing attacks on a private network. It involves the routing device interconnecting the private network to a public network, where the incoming data is matched against patterns belonging to known attacks associated with private networks. The source of the data packets is then designated as either being malicious or authentic, depending on the diagnosis of the data packet. This allows the routing device to identify both the DoS and address spoofing attack and take preventive measures by identifying the attacker by tracking the packet’s information. This way, both DoS and address spoofing can be blocked. Adrienne Porter Felt and David Wagner et. al. [8] assess the risks of phishing on mobile platforms. The mobile OS and browser lacks secure application identity indicators, so it is not always readily identifiable whether a link has taken the user to an unexpected application. They state that phishing attacks have become more common as users nowadays have grown more accustomed to entering passwords in familiar settings. A study found that websites and mobile applications commonly link to password protected sites like social networking sites or payment gateways. This conditions the users to reflexively enter password after following links. It can be demonstrated that it is possible to build phishing attacks that can imitate the links and steal the data. Further tests show that many of the attacks happen without user detection. Jamal Raiyinet. al. [9] discusses and carries out comparisons between different cyber attack detection strategies. The techniques have been improved upon drastically over time, but developing new attack detection schemes is necessary because cyber attackers are constantly developing. Traditional cyber attacks detention has its limitations, such as only being able to detect known attacks. Security experts may also have to manually analyze attack related data and come up with new specifications. Most systems focus on data produced by a single source. A technique is proposed which is based on adaptive agents, and the cyber immune system is based on behaviour analysis. P. Ferguson and D. Senieet. al. [10] state that the DoS attacks that have used forged addresses have proven to be a troublesome issue. The resurgence of these types of
attacks have pushed network providers to find new and improved protection methods to curb these attacks. They propose methods involving traffic filtering, which reduces the effectiveness of source address spoofing DoS attacks. Service providers have already started implementing this type of filtering. This method, in addition to defeating this attack, can also help track the source of the attack. As address spoofing is meted out, it becomes easier to track the attacker as the attacker’s address is more likely to be valid. As the number and frequency of attacks decreases, more resources will be available for tracking the attacks which may occur.

Arun Kumar Yadav and Karan Singh et. al. [11] discuss various routing protocols involved in Mobile Adhoc Networks in order to overcome the known drawbacks, this is because the subject is still under study and it is not certain that all the drawbacks are known. These known drawbacks include the extent of how authentic data is, integrity of data, security of the packets passed between layers and confidential nature of data. The paper specifies the possible attacks on each layer in the manet and also distinguishes them as internal and external, active and passive, and finally also specifies the routing protocols that can be used in order to avoid these attacks: SEAD, ARIADNE, SRP, ARAN, SAR, SOADV. Each protocol’s implementation is elaborated. To summarize it can be said that this paper is to bring the reader up to date on security issues with respect to MANETS and also give details in how to implement better routing protocols to overcome drawbacks and avert attackers.

Mohan V. Pawar, Anuradha J. et. al [12] describe the independent nature of nodes in a MANET network and their ability to freely move around and goes on to explain the security issues present with this sort of arrangement. The authors of this paper present some of the possible ways in which an attacker can turn one of the nodes in the network to a malicious node and take advantage of the salient features of a MANET arrangement. They describe the node in a MANET network as a selfish entity as it can utilize or take advantage of the resources of another node and keep its own resources in-tact. They also claim that the precautions to be taken by users and administrators of an adhoc network is to install operating system updates periodically, keep an up to date antivirus and also to restrict each system on the network instead of allowing all that it asks for.

Salah Alabady et. al. [13], in his paper, implements a security system for a network by using a router and firewalls, however, it also describes the vulnerabilities of such a system i.e., systems that use firewall and router. The authors conduct an in-depth study on the possible attacks on this system and also provided a checklist of what to do in order to protect ones network from the attacks aforementioned. The policies of the firewall are inspected and ideal policies are described i.e., for optimal results.
Swati Bartariya and Ashutosh Rastogi et al. [14], highlight the threats present in using a wireless sensor network and suggesting some ways to overcome these and avoid attacks on the users of the network. In this paper, there is a description of the various forms of sensor networks, the applications and architecture. It contains detailed description of the various attacks that are capable to harm and cripple this network. It is suggested to resolve the security issues by using cryptography and keys.

Jyoti Thalor and Ms. Monika et al. [15], in their paper, aim at bringing out the effects of a wormhole attack on a MANET, to identify the existing ways to prevent this and identify it. It also giving us new ways to prevent and identify these attacks. Various methods are listed and compared in a tabular format in order to be most informative. Finally it is concluded that there is no one solution and depending on the situation different solutions may be presented.

Rajinder Singh, Parvinder Singh, and Manoj Duhanet al. [16], bring forth that in recent times mobile adhoc networks or MANETS have emerged as the hot topic for researchers, the authors for this paper have successfully implemented this and showed us how this can be done practically by using a certain approach - security based algorithm. They identified the most significant threats to a MANET (i.e., all possible attacks-active and passive). Based on a survey of the likely threats, each approach to implement the network is listed which means that to avoid each attack which approach to implement is appropriate. A step by step proposed solution to prevent the wormhole attack. The paper also contains an explanation of the implemented architecture of the MANET and its advantages, with a step by step procedure on how to implement.

5. Mitigation Strategy : measures to improve Network Security

- **Online Anti-Virus Measure:** The network manager's task is to monitoring the prevention mechanism. Previously, the installation of the anti-virus software (such as rising anti-virus software) was mandatory for all the users. But later it was found that, this approach has some limitations as the users have limited computer skills.

- **Measure to prevent hackers:** Invasions and attacks can be distinguished into two types of issues; subjective security issues and objective security issues. The errors, which are made by ant network management personnel are dealt by Subjectivity security issue. The hackers try to perform various types of attacks by figuring out the loopholes in network security protocol. This type of severity belongs to Objectivity security issues.
• **Use safety tool:** To install the patch on time, the network manager has to check all the security issues need frequently. The use of the scanning tools by the network manager to scan the host machine and to find out the feeble links and based on this measures, he/she may take some appropriate preventive actions.

• **Firewall technology:** Firewall works like a shield, which prevent the outsiders from accessing one's network device. Packet filtering technology, Agent technology, and Status monitoring technology- these are the three variants of this firewall technology. To verify any IP address by setting it, Packet filtering technology is used. The firewall filters out all those IP addresses which do not match those setting and provides first layer of protection. To verify the authority of any requests, transmitted by the proxy server clients, Agent filtering technology is used. Mainly this technology focuses on the user authentication, filtering criteria and protecting the internal IP addresses. To effectively monitoring all levels of network- Status monitoring technology is used which is the third generation of the network security technology. This enables the making of timely security decisions.

6. **Conclusion**

In this paper, various kinds of attacks are being discussed to identify the loopholes in the network security. Each of the issues is being analyzed and best possible mitigation strategy is provided against it. It is being observed that the use of SSH keys (secure shell keys) will prevent the intruders from unauthorized access to any network. Proper isolated execution environment is required to mitigate this severe attacks. On the whole, the proposed strategies performs quite effectively and there is scope for its further improvement.

7. **Acknowledgements**

The project would never have been successfully carried out without the help of our respected guide Prof. Siva Rama Krishnan S Sir. Because of his guidance and support only, the paper is where it is now. Besides that, we are thankful to all the VIT University provided facilities. Those are the factors which made the whole process smooth and free of hurdles.

**References**
