IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Intrusion Detection For Known And Unknown Security Attacks

Dr.Md.Yusuf Mulge
PDM College of Engineering for Women, Bahadurgarh, Haryana, India
dryusufmulge@gmail.com

Abstract

Internet has enabled us to connect to any computer, at any time from any geographical location. But at the same time there is possibility of security attacks. However, security attacks are not limited only to the Internet; attacks can even be on our own local area network (LAN) or wireless LAN. As networks were actually created to share information among users and other services, some network administrators never strove for higher security measures. In fact in some cases, network security was compromised for easiness in sharing files or for remote access/control like enabling file sharing, SNMP (Simple Network Management Protocol) etc. Due to Internet large number of users are vulnerable to network attacks, as they are not familiar with different types of network attacks. Since firewalls and other self-protective security measures are not sufficient, you need supplementary tools to detect and respond to security breaches as they take place.

Introduction

A network monitor along with Intrusion Detection System can detect known (and even some unknown) network attacks and make the prevent procedure much more efficient and present the results in a human-readable report [1].

In this research we have focused on the common types of attacks that any network may undergo and also ways through which they can be detected. We have also highlighted some of the weaknesses of the current defense mechanism like firewall, and we have included some suggestions that may be used to improve the current defense tools by changing its architecture and policy [2].

This paper is organized as follows:

Section 2 is on the network attack classification,
Section 3 is on identifying a compromised system,
Section 4 is on misconceptions on firewall,
Section 5 is on some network attacks done,
Section 6 is on some safeguard measures to be taken,
Section 7 is on DoS (Denial of Service) attack countermeasure using IDS/IPS and
Section 8 is the conclusion.

Calcification of Network Attack

The following descriptions of network attacks are grouped by attack – the network protocol-based attack, host-based attacks and attacks on network application layer [3] –[5].

A. Network Protocol Intrusions

The following attacks take place because of the flaws in networking protocols or flaws in software that implement the networking protocols. And those intrusions concentrate on network & transport layer of the OSI Layer.

Host & Port Scanning – Attackers usually use one of these techniques to identify hosts for further examination, which includes network scanning, ping broadcast and Denial of Service. Attacks may loop through the possible IP addresses for systems and send an ICMP echo request to each address. The broadcast ping has two main uses for attackers – one is to identify all hosts on the target subnet and the second is to create a denial of service by amplifying single, frequent ping request. This may generate many more ICMP echo responses that may create temporary traffic congestion in the network that slows down the whole network and make the target computer inaccessible via the network. Attackers often also use port scanning after identifying a valid host to identify TCP and UDP services that are being offered by that particular host. In most cases, the attackers try to hide the true source IP address of the attack with decoys which can simultaneously generate matching scanning packets with other source IP addresses. Common types of port scanning includes, TCP SYN Port Scanning, TCP Stealth Port Scanning and UDP Port Scanning etc. During our test we have used NMap and WiP which are both very powerful tool for port scanning.

DNS Spoofing & Cache Poisoning – DNS Spoofing is where the attacker makes a DNS entry to point to another IP address than it would be generally

pointing to. It works stealthily by unknowingly forcing a victim to generate a request to the attacker's server, and then spoofing the response from that server. An attacker can predict what request that victim server will send out to satisfy a web client's request, and can spoof the response, which will arrive before the real response arrives. Generally, DNS servers would cache information for a certain time period. If an intruder can successfully poison the cache and spoof a response for "www.some-known-website.com", any normal users of that DNS server will then be redirected to the intruder's website. DNSA is a free tool for DNS auditing and spoofing that we tested on an Ubuntu 4.2 unix based machine.

Web Spoofing – Web Spoofing permits an attacker to observe and change all the web traffic sent to the victim's machine, and capture all data entered into the web page forms (if any) by the victim. This happens even when the browser connection shows the secure sign and the user is totally ignorant of what is happening. The attack can be done using Web plug-ins and JavaScript segments. The attack once implemented is started when the victim visits a malicious web page through a web link in a malicious email message sent by the attacker. Once the victim responds, the attacker causes a browser window to be created on the victim's machine through forgery, by imitating genuine websites. Then, the attacker causes all the web traffic destined for the victim's machine to be routed through the attacker's server.

Email Spoofing – Email spoofing is the practice of changing one's identity in email address so that it looks like an email that came from a trusted source or from someone else. Spammers normally employ this approach to conceal their identity. Since SMTP servers generally requires no authentication, it is very easy to change the original email address to a forged one, that can eventually fool the victim into performing some sensitive steps indicated in the email.

Session Hijacking – TCP session hijacking occurs when the attacker takes control over an active TCP session between two computers. Since most authentications only happen at the start of a TCP session, this allows the attacker to gain access to a computer.

A popular method is using source-routed IP packets. This allows an attacker at PC A on the network to participate in a conversation between PC B and PC C by encouraging the IP packets to pass through its machine. If source-routing is turned off, the attacker can use "blind" hijacking, whereby it guesses the responses of the two machines. Thus, the attacker can send a command remotely, but can never see the actual response.

However, a common command given would be to set a password allowing remote access from outside the network. The attacker can also be "inline" between B and C using a sniffing program to watch and capture their packets. This is often termed as a "man in the middle attack". A common module of such an attack is to execute a denial of service (DoS) attack against one end-point to stop it from responding. This attack can be either used against the target computer to force it to crash, or against the network connection to force heavy packet loss due to excessive traffic congestion.

Ping of Death (Long ICMP) – Ping of death also known as “long ICMP” is a type of denial of service (DoS) attack caused by an attacker intentionally sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; which allows a single IP packet to be broken down into smaller chunks. In past attackers used to take advantage of this loophole when they figured that a packet if broken down into small chunks could add up to more than the allowed 65,536 bytes. Many OS in past didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted. Ping of death attack was very nasty because the identity of the attacker could be easily spoofed; the attacker didn't need to know anything about the target machine except for its IP address. By the end of 1997, the major OS vendors came out with patches to overcome the issue of oversized packets. Still, many Web sites continue to block Internet Control Message Protocol (ICMP) ping messages at their firewalls to prevent any future variations of this kind of denial of service attack. Some machines prior to Windows 2000 are still vulnerable to this attack..

Other Attacks – There are many other attacks that falls under OSI network and transport layers, they are – DNS Zone Transfer, Ftp Bounce, Finger, Forged Invalid IP Fragment (Teardrop), TCP SYN Spoofing, Daemon Buffer Overflows , Forged Invalid TCP SYN, Out of Band TCP Data, Simple UDP Services Bounce, NFS File Handle Guessing,
RSH SYN Spoofing etc.

B. Host Intrusion Intrusions which attack host operating system are discussed here:

Password Sniffing – An attacker may install a password sniffer to obtain passwords for accounts on other systems. Telnet, FTP, POP, and other authenticated network protocols usually transmit passwords as clear-text. Many software offers facilities to sniff, such as the Berkeley Packet Filter or Ethereal which can be used to hear all traffic on the network to which the system is attached. Password sniffing programs use this eavesdropping

facility to listen to the first few bytes of each network connection. The overheard information is saved to a file and transmitted to another host for storage. A hacker can use the passwords to gain access to accounts on other systems.

Remote Backdoor Access – A hacker who has somehow gained a onetime access to a system may install a "backdoor" program that will allow privileged access to the system in the future from a remote location. This may be particularly very useful for the hacker if the system administrator closes the original hole that was used to compromise the system or if the original exploit required a large investment of time or work. The hacker may also use the backdoor to provide easy access for other intruders.

Disabling Security Options – If an attacker gets access to a target terminal, he may also disable the common security options such as – firewall, IDS (Intrusion Detection System) which will leave the target vulnerable. Sometimes viruses and Trojans are used to dysfunction these security services. Other intrusions which attack host operating system are Password Guessing, Social Engineering, Temporary File Traces, Reading or Writing Critical Memory, Trojan and viruses, Removing system/security log etc.

MAC Spoofing – In this attack, an attacker spoofs his original MAC address to the MAC address he wants to spoof. This attack can easily be launched with MAC spoofing tools such as Mac Makeup software. An attacker can learn the MAC address of the valid user by capturing wireless packets using any packet capturing software by passively or actively observing the traffic. It was observed that upon successful MAC spoofing, besides the spoofed MAC address, the IP address assigned to the attacker's computer was identical to the IP address of the victim computer, whose MAC address was being spoofed, because of the ARP (Address Resolution Protocol) protocol in a network.

IP Spoofing – IP spoofing is a process used to gain unauthorized access to computers, whereby the attacker sends packets to a computer with spoofed IP address implying that the message is coming from a trusted and genuine host. To implement IP spoofing, an attacker must first capture packets to find the IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. IP spoofing forms a basis for various other network attacks. But newer security enabled routers and firewall filters can stop IP spoofing.

C. Network Application Layer Intrusion

Those known intrusions that target network application layer and their details are numerous. They are: Sendmail debugging commands, Unauthorized use of NFS, Trivial File Transfer Protocol, Use of rlogin or rsh from untrusted hosts, RPC Portmapper Proxy, Insecure Web Server CGI Programs, Microsoft Internet Information Server (IIS), NT NULL Session and many more.

Identifying a Compromised System

A.Background of Problem

When one of the terminals on our network has been compromised, we need to identify the issue fast enough before the attacker actually does any major harm on the network [6]. One of the ways is to use a normal network monitor or analyzer as a security and monitoring tool on your network. In reality, one's firewalls or OS won't release a patch until the damage is already been done somewhere. Imported disks drives, deliberate actions by ones employees and visitors bringing infected terminals (e.g. laptops) to connect to the network are actually some of the key weak spots in the network that the common perimeter defense cannot cater for all alone. A good network analyzer or monitor with an intelligent IDS (Intrusion Detection System) capabilities can help us to detect when a breach of security has occurred and also make our recovery process much easier

B.Solution

Attacks and also viruses often generate a recognizable pattern or 'signature' of packets after performing an attack on the network. A network analyzer coupled with an intelligent Intrusion Detection Software (see section VII) can identify these packets as noted before and alert the administrator about the attack via email or SMS. Most of the network analyzer or monitors now a days can let us set alarms to be triggered when a particular set of patterns are seen. If communication technologies are embedded with the network analyzer, it can be easily programmed to send an email or an SMS when a particular type of condition is met.

Misconception About Firewalls

There is a common misconception among many computer users that makes them believe that having a "firewall" is simply the end of all sorts of network security breaches. But this is indeed not true and believing this may be very costly [7]-[8]. It is in fact a misunderstanding on the way firewall works.

A firewall basically monitors the connections and packets that are going in and out from one's computer. If the packets are of acceptable 'type' as per the policy, it will be allowed; anything other than that will be blocked and terminated. But what if the hacker actually doesn't directly attack one's pc? Instead he stays in the middle of two computers and captures the packets in between?

During our testing we have intercepted chat conversation performed by MSN Messenger, Yahoo Messenger & ICQ of two wireless terminals which were both protected with Windows Firewall. We were also able to change the content of the package as it was being sent to the receiver.

Some Network Attacks Done

We were able to crack the Cisco Router Password of our experimental network using Cain & Abel software. We were able to capture the packets which were sent using Msn Messenger (Port 443). We were able to capture packets using Ethereal in Local Area Network and look for machine details. We were able to crack down the WEP encryption key and WPA-PSK. ARP Poisoning was done using Cain & Abel software. The second laptop couldn't access the local network and the Internet, while we were poisoning. When we used telnet to communicate with the Belkin Router, the password could be captured (as it is sent in the clear). Attack was done on the mail server to do a brute force attack to guess passwords for usernames and the server was allowing such incorrect guesses a multiple number of times. We used Brutus which is one of the fastest, most flexible remote brute force password crackers as shown in fig. 1. It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB Telnet, IMAP, NNTP etc. We also did port scanning to see open ports and to find other details. With Net Ranger software, it's fairly simple to get detailed information of our network. For instance – current active connections, active ports, foreign addresses and so on. MegaPing software has multi functionalities such as – NetBIOS Scanning, Port Scanning, Host Monitor, Trace route, Finger etc. Figures 1 to 7 show some of the attacks done.

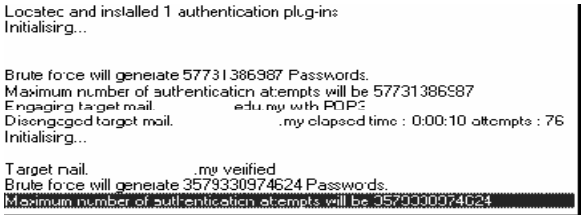

Fig.1 BRUTUS software doing a brute force attack for passwords on an email server (some lines and figures are deleted for privacy)

The fig.2 and fig.3 show how Aircrack 2.1 software was used to crack a 40 bits and 128 bits WEP keys respectively of a wireless network. Other WEP cracking software includes WEPCrack and WEPLab etc.

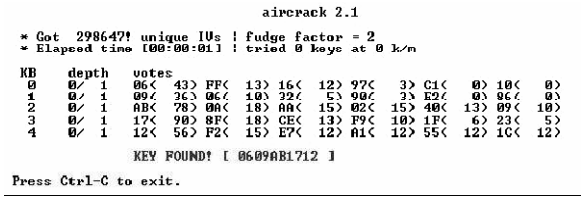

Fig.2 Cracking 40 bits alphanumerical WEP static key in a WLAN.

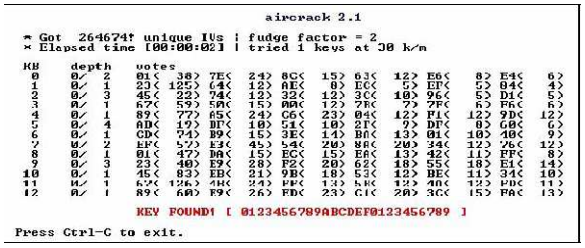

Fig. 3 Cracking 104 bits alphanumerical WEP static key in a WLAN

Here sufficient number of wireless packets was captured and the WEP cracked using the cracking software. Attack on WPA (WiFi Protected Access) can also lead to the following result as in fig. 4, where the WPA pass-phrase (PSK) can be recovered [9].

$ ./cowpatty -r <libpcap file> -f <dictionary file> -s <SSID info>

coWPAtty 2.0 - WPA-PSK dictionary attack.

Collected all necessary data to mount crack against passphrase.

Loading words into memory, please be patient ...
Done (11200 words).

Starting dictionary attack. Please be patient.

[1000] [2000] [3000] [4000]

The PSK is "hello my world".

3123 passphrases tested in 97.55 seconds: 32.01 passphrases/second

Fig. 4 Sample WPA-PSK dictionary attack for pass phrase (PSK).

Fig.5 shows that the network scanning has shown severe security problem with a computer that involves administrator login without a password.

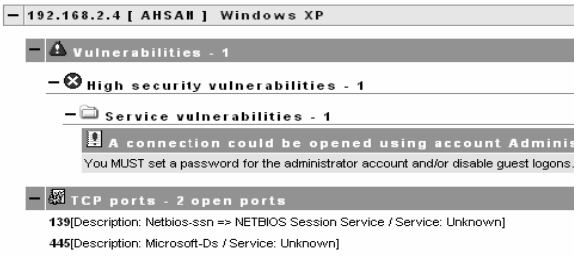

Fig. 5 Network scanning reveals that the computer has an administrator login without password.

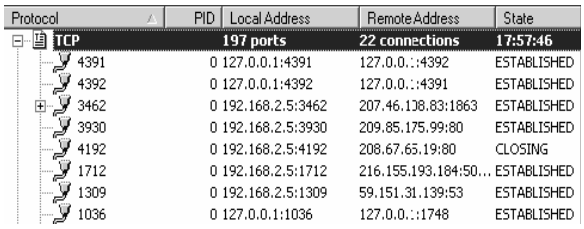

Fig. 6 MegaPing has multi functionalities such as – NetBIOS Scanning, Port Scanning, Host Monitor, Trace route, finger etc, shows IP and port details. Fig.6 shows how to get network information like open ports and IP addresses using a specific tool which can be used for attacks later.

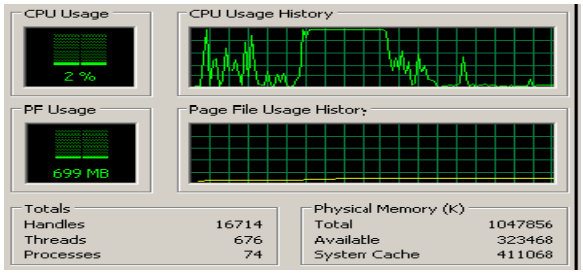

Fig. 7 shows the DoS attack performed using the ping command from multiple sources using the command – "ping –t <IP address of target>". It eventually drowned the target PC where the CPU usage hit 100% and used up memory and page files.

General safeguards On Network Security

A. Wireless Network

Based on our overall test result we have seen that wireless networks are more vulnerable to attacks. There are several basic things that we may do, to provide some 'basic' security to our wireless network [9].

They are as follows:

Changing the network SSID.
Turning off SSID
Protecting the intranet
MAC Based Authentication
Enabling WPA encryption instead of WEP
Enable mutual authentication
Disabling Remote Administration

B.Wired Network

Wired networks are safer compared to the wireless networks as it requires the attacker to be connected to the network physically if he is unable to break though the network from a remote location. Other than the basic measures that we may have already implemented, below we have listed some of the key areas which many network administrators overlook.

Secure Wall Mounted Ethernet Port
MAC Based Authentication

Countermeasure Against DoS Attacks Using Intrusion detection/Prevention System

We propose a general architecture for an Intrusion Detection or Prevention System, especially against flooding attacks (DoS attacks) or other variants, which can be as shown in the flow chart of figure 8.

It deals with monitoring the attack signatures and comparing it with an existing database of attack signatures. If the attack signature is found, then it is stopped and warning issued to administrator. As an improvement, fine tuning can be done with the ability for self learning and correcting false decisions through statistical approach/ AI approach as it lives longer in the network. Initially, test installation can be done and a variety of mock DoS attacks can be performed. During the test period (say, *n* months), the suspicious attacks are only alerted to the administrator. When satisfactory attack reaction results are obtained, it can be installed and made active. The attack signature database is updated online in regular intervals to keep it up-to-date. Some customization can be implemented so that an administrator can set in additional network threshold values. Once the threshold values are crossed, some specific action is taken. To avoid false positives, the system needs to be trained and the optimal values should be set after that[11].

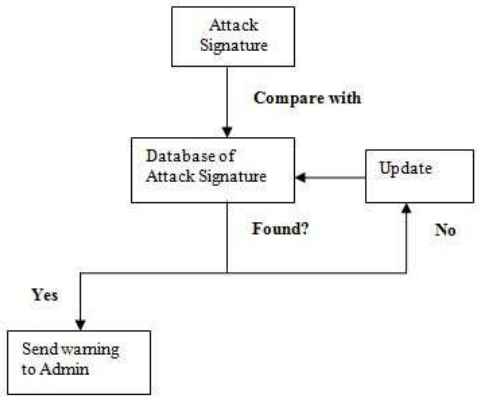

Fig.8 General Intrusion Detection or Prevention Architecture Flow chart.

Conclusion

From above observations it is very clear that, wireless networks are vulnerable to attacks. Therefore some basic care need to be taken. On the other hand wired networks needs physically connection to be intruded. Hence they are safer as compared to wireless networks.

References

[1] M. Crosbie and E. H. Safford, "Defending a Computer System Using Autonomous Agents", Technical Report No. 95-022, Dept. of Computer Sciences, Purdue University, IN.

[2] J. McHugh, A. Christie, and J. Allen, "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software*, Oct 2000.

[3] M. Malkin, T. Wu and D. Boneh, "Building intrusion tolerant applications", *Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX '00)*.

[4] Symantec and I. Poynter, Jerboa Inc. "Quantifying Vulnerabilities in the Networked Environment: Methods and Uses Char Sample", 2000.

[5] C. L. Schuba, "Analysis of a denial of service attack on TCP," *Proc. Of IEEE Security and Privacy Conference*, pp. 208-223, 1997.

[6] Anti-Phishing Working Group, Retrieved on 12 June 2007, Available online at http://www.antiphishing.org

[7] ICQ Threat, Retrieved on 16 June 2007, Available online at http://www.symantec.com/region/tw/enterprise/article/icq_threat.html.

[8] M. Walton, "Five ways to secure your organization's information systems", Retrieved on 15 June 2007, Available online at http://articles.techrepublic.com.com/5100-10878-1060329.html, 2001

[9] Takehiro Takahashi, "WPA passive dictionary attack overview (White Paper)", 2004.

[10] Home and Small Business Networking, "Improve the security of your wireless home network with Windows XP", Retrieved on 16 June 2007, Available online at http://www.microsoft.com/windowsxp/using / networking/security/wireless.mspx

[11] L. A. Mohammed, B. Issac, "Detailed DoS attacks in wireless networks and countermeasures", *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*

Abbreviations

ASIC	Application Specific Integrated Circuit
DDOS	Distributed Denial of Service Attack
DFA	Deterministic Finite Automaton
DNS	Domain Name System
DoS	Denial of Service
FIRE	Fuzzy Logic Rule Engine
FPGA	Field Programmable Gate Array
FTP	File Transmission Protocol
ICMP	Internet Control Message Protocol
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IMAP	Internet Message Access Protocol
IP	Internet Protocol
MIND	Minnesota Network Intrusion Detection
NFA	Non-Deterministic Finite Automaton
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
OSHBIDS	Open Source Host-based intrusion detection system
POD	Ping of Death
SPADE	Statistical Packet Anomaly Detection Engine
TCAM	Ternary Content Addressable Memories
TCP	Transmission Control Protocol