COUNTERMEASURE TOOL - CARAPACE FOR NETWORK SECURITY

Anand Bisen[1], Shrinivas Karwa[2], B.B. Meshram[3]

[1,2,3]Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai, MH, India

[1]anandbisen2008@gmail.com, [2]shrikarwa1@gmail.com, [3]bbmeshram@vjti.org.in

Abstract

Now a day frequency of attacks on network is increased. In this, denial of services (DOS) and IP spoofing are more common. It is very difficult to find out these attacks.

Denial of services (DOS) and its type Distributed denial of services (DDOS) are significant problem because it is very hard to detect it. Its main aim to shut resource from internet, and make resource unavailable to legitimate users. IP source address forgery, or "spoofing," is a long-recognized consequence of the Internet's lack of packet-level authenticity. IP spoofing is very powerful when it implemented with Distributed denial of services (DDOS).

In this paper we deal with the information gathering process to do attacks. The information gathering about the weaknesses of the target system and helps to do attack. Lastly we proposed a new model to protect from attacks.

Keywords

Distributed denial of service (DDOS), IP spoofing

1. INTRODUCTION

The Internet was originally designed for openness and scalability. The infrastructure is certainly working as envisioned by that yardstick. However, the price of this success has been poor security. For example, the Internet Protocol (IP) was designed to support ease of attachment of hosts to networks, and provides little support for verifying the contents of IP packet header fields [Clark 1988]. This makes it possible to fake the source address of packets, and hence difficult to identify the source of traffic. Moreover, there is no inherent support in the IP layer to check whether a source is authorized to access a service. Packets are delivered to their destination, and the server at the destination must decide whether to accept and service these packets. While defenses such as firewalls can be added to protect servers, a key challenge for defense is how to discriminate legitimate requests for service from malicious access attempts.

If it is easier for sources to generate service requests than it is for a server to check the validity of those requests, then it is difficult to protect the server from malicious requests that waste the

DOI : 10.5121/ijnsa.2011.3302

resources of the server. This creates the opportunity for a class of attack known as a denial of service attack.

When the traffic of a DoS attack comes from multiple sources, it is called a *distributed denial of service (DDoS) attack. By using multiple attack sources, the power of a DDoS* attack is amplified and the problem of defense is made more complicated.

A typical DDoS attack contains two stages as shown in Figure 1.

The first stage is to compromise vulnerable systems that are available in the Internet and install attack tools in these compromised systems. This is known as turning the computers into “zombies.”

In the second stage, the attacker sends an *attack command to the “zombies”* through a secure channel to launch a bandwidth attack against the targeted victim(s).

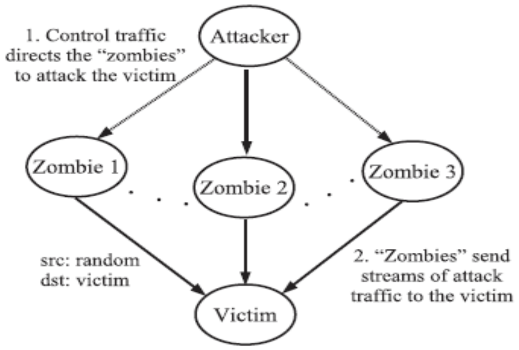


Figure 1: Structure of a typical DDOS attack

IP spoofing is about the most advance trick or attack that can be executed on a computer system. Almost any aspiring computer hacker would be proud of being able to spoof their IP address and fool the target system into establishing illegitimate connection. IP spoofing happens when an attacker tricks or bluffs the target system into believing that data packets being sent to them started from a source other than a actual source system.

Suppose there attacker with IP address 111.11.111.11(Real), it send packet to a victim with IP 222.222.22.222(Victim) and there is a fake IP 33.333.33.333 so in normal condition if attacker send a packet to victim then source address is real IP address but in IP spoofing victim find that packet come from fake IP address.

The rest of the paper is structured as follows.

In section 2 we find out the information that is needed for attack in this section we discuss method to find out IP address, in section 3 we discuss how this information is useful for attacker to do attacks, in section 4 with help of information and tools we perform attack and in last we proposed a model that helps to protect a system from attacks.

2. PREPARING FOR ATTACK

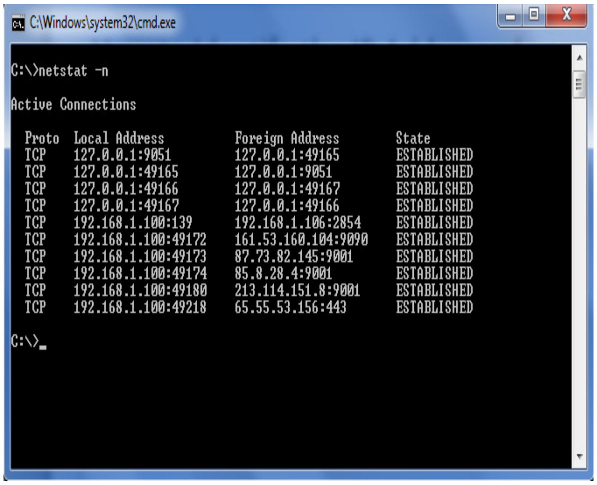
Before attacking, it is important to find out information about victim system. IP address, OS, firewall detection, list of open ports and list of services are more important.

Table 1: Information and tool

Information Gathering	Tool / Mechanism
IP Address	Through Instant Messaging Software Through E-Mail Header
Firewall	Traceroute command is used to find out firewall.
Operating System	To find out operating system of target machine fingerprinting is used
Hop Count	With the help of initial TTL and final TTL value we can find out hop count.
Geographical location	Neo trace is tool that is use to find geographical location of target system
Ping Sweeping	Fping is used
Port number	Nmap tool is used to find number of open ports of target systems.

2.1. IP address

An IP address is a 32 bit decimal number that is normally written as four number between 1 and 255(8 bits, or 1 byte each) ,each separated from the other by a decimal point. To identify IP address we can use netstst –n command (in figure 2).



```
C:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:9051         127.0.0.1:49165        ESTABLISHED
  TCP    127.0.0.1:49165        127.0.0.1:9051         ESTABLISHED
  TCP    127.0.0.1:49166        127.0.0.1:49167        ESTABLISHED
  TCP    127.0.0.1:49167        127.0.0.1:49166        ESTABLISHED
  TCP    192.168.1.100:139      192.168.1.106:2854     ESTABLISHED
  TCP    192.168.1.100:49172    161.53.160.104:9090    ESTABLISHED
  TCP    192.168.1.100:49173    87.73.82.145:9001      ESTABLISHED
  TCP    192.168.1.100:49174    85.8.28.4:9001         ESTABLISHED
  TCP    192.168.1.100:49180    213.114.151.8:9001     ESTABLISHED
  TCP    192.168.1.100:49218    65.55.53.156:443       ESTABLISHED

C:\>_
```

Figure 2: netstat command

The IP address shown in the local address field denotes the IP address of your system. In this case the IP address of local system is **192.168.1.100.** There is some more method to find out IP address such as

2.1.1. Through Instant Messaging Software

The most common technique of enumerating the IP address of remote system is through Instant messaging software like ICQ, MSN messenger, Yahoo messenger and so on.

1. ICQ

I seek you or ICQ is among the most popular chatting software around. In this whenever you start a chat session with friend in ICQ, a direct connection between both of you is opened by the ICQ software with the help of ICQ server. Assume that your IP address is xx.xx.xx.xx and your friend have yy.yy.yy.yy then messages are transfer in following manner

xx.xx.xx.xx ←-------→ yy.yy.yy.yy

You can find out IP address of any ICQ user even if IP hider has been enabled by following steps:

- Launch MS-DOS.
- Type netstat –n command to find out the open ports and IP address of the machine with which a connection has been established.
- Launch ICQ and send message to victim.
- While you are chatting, return to MS-DOS and issue the command netstat –n. You can find out new IP address this will probably the victim's IP address.

2. Other Instant Messengers

Whenever you start a chat session with a friend on the other instant messenger like MSN, an indirect connection between you and your friend is opened via MSN server. So all communication take place via MSN server.

xx.xx.xx.xx←-- →MSN server←---→yy.yy.yy.yy

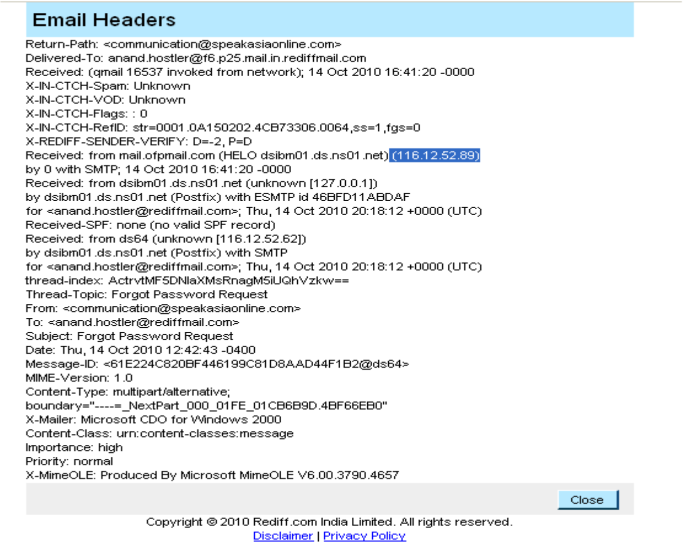
So whenever you issue netstst –n command it doesn't give your friend's IP, instead it give IP of server. So to get IP of victim sender will get by sending file. **Steps:**

- Start chat with victim.
- Use MSN messenger's in-built file transfer feature to send a file to victim.
- When victim accepts the file transfer and the transfer process starts, launch netstat –n command. It give IP of victim because for transferring file direct connection between sender and victim exists, there is no intermediate server.

2.1.2. Through E-Mail Header

The e-mail headers of every single e-mail sent on the Internet contains the IP address of the person who sent that particular e-mail. Hence, each time you receive an e-mail, you can easily study the e-mail headers to reveal the identify of the person who actually sent that particular e-mail. **Steps:**

- Open email header
- Identify IP address of the computer that was used to send the e-mail.



```
Email Headers
Return-Path: <communication@speakasiaonline.com>
Delivered-To: anand.hostler@f6.p25.mail.in.rediffmail.com
Received: (qmail 16537 invoked from network); 14 Oct 2010 16:41:20 -0000
X-IN-CTCH-Spam: Unknown
X-IN-CTCH-VOD: Unknown
X-IN-CTCH-Flags: : 0
X-IN-CTCH-RefID: str=0001.0A150202.4CB73306.0064,ss=1,fgs=0
X-REDIFF-SENDER-VERIFY: D=-2, P=D
Received: from mail.ofpmail.com (HELO dsibm01.ds.ns01.net) (116.12.52.89)
by 0 with SMTP; 14 Oct 2010 16:41:20 -0000
Received: from dsibm01.ds.ns01.net (unknown [127.0.0.1])
by dsibm01.ds.ns01.net (Postfix) with ESMTP id 46BFD11ABDAF
for <anand.hostler@rediffmail.com>; Thu, 14 Oct 2010 20:18:12 +0000 (UTC)
Received-SPF: none (no valid SPF record)
Received: from ds64 (unknown [116.12.52.62])
by dsibm01.ds.ns01.net (Postfix) with SMTP
for <anand.hostler@rediffmail.com>; Thu, 14 Oct 2010 20:18:12 +0000 (UTC)
thread-index: ActrvtMF5DNlaXMsRnagM5iUQhVzkw==
Thread-Topic: Forgot Password Request
From: <communication@speakasiaonline.com>
To: <anand.hostler@rediffmail.com>
Subject: Forgot Password Request
Date: Thu, 14 Oct 2010 12:42:43 -0400
Message-ID: <61E224C820BF446199C81D8AAD44F1B2@ds64>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_01FE_01CB6B9D.4BF66EB0"
X-Mailer: Microsoft CDO for Windows 2000
Content-Class: urn:content-classes:message
Importance: high
Priority: normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4657
```

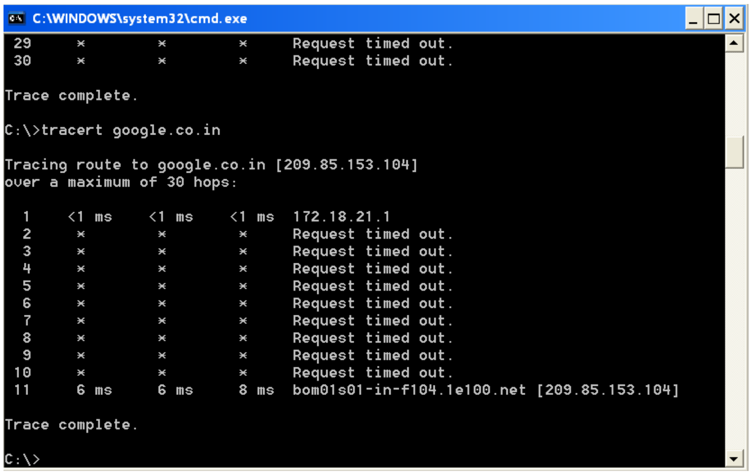
Copyright © 2010 Rediff.com India Limited. All rights reserved.
Disclaimer | Privacy Policy

Figure 3: Email Header

So from header we can get IP address of the e-mail in this case is **116.12.52.89** (in figure 3).

2.2. Determining Firewall

You can often use the traceroute to detect the presence of a firewall on the target system's network. To do so, simply examine the output of the traceroute command please refer figure 4. If you find asterisk (*) in the output, it means traceroute has timed out. As ingle instant of such a timeout does not necessarily confirm the presence of firewall. However several instances of time indicate the presence of firewall on target system's network.



```
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\>tracert google.co.in

Tracing route to google.co.in [209.85.153.104]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.18.21.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     6 ms     6 ms     8 ms  bom01s01-in-f104.1e100.net [209.85.153.104]

Trace complete.

C:\>
```

Figure 4: Determining Firewall

2.3. Operating System Detection

It is very import for an attacker to determine the operating system running on the target host. One of the easiest methods to find that you can use for operating system detection is fingerprinting, which art of comparing data packet is sent by the target system to already known values in order to determine the operating system. There are two types of fingerprinting:

- Active fingerprinting
- Passive fingerprinting

Active fingerprinting: we know that different operating systems respond differently to the same kind of ICMP message. This means that once we have learned how the various operating systems respond to specific type of message, we can use this knowledge to determine operating system of target system. All types of packet can be used for active fingerprinting purpose:

- ICMP error message quoting
- ICMP error message quenching
- Assessing ICMP error message
- Assessing the initial windows size
- Flag probe
- Studying the ACK value
- Studying initial sequence number
- Sending FIN packet to open ports on the remote system
- Don’t fragment
- Window size

In this method TTL value plays a major role in the functioning of traceroute command. It is important to note that such TTL values can also be used to determine the operating system of remote system. In table 2 we give TTL value against operating systems.

Table 2: Default Initial TTL Values Used by Various OS

Operating System	Default TTL Value
Windows	32
AIX	60
Cisco	255
Red Hat 9	64
Solaris	255
HPJetDirect	59
DC-OSx	30

Steps to find out OS:

- Using trareroute determine the number of hops (router) between your system and target system.
- Determine the final TTL value of a data packet sent by the target system to your system.

- Add the number of routers between your system and target system to the final TTL value of packet send by target system to your system.
- Once you have initial TTL value from table you can find out the Operating system on target system.

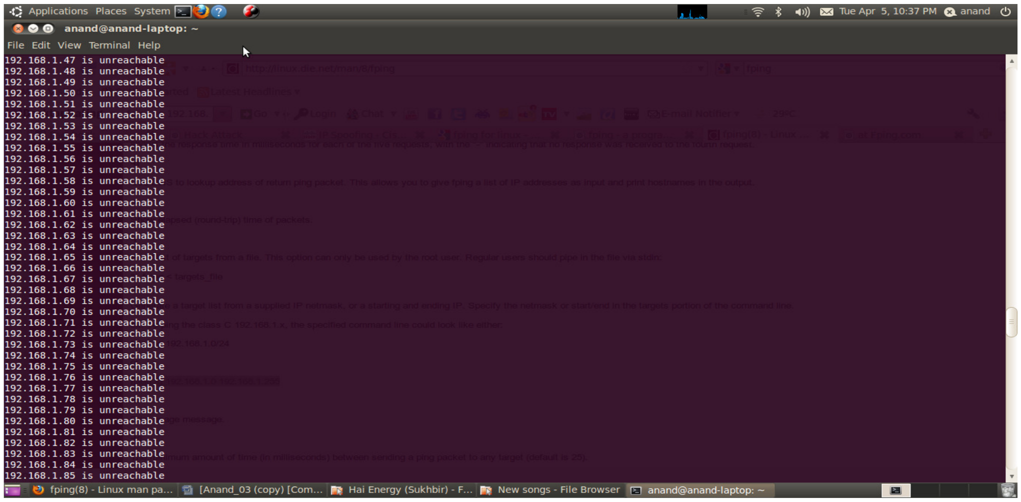
Passive fingerprinting: like active fingerprinting, passive fingerprinting is based on the fact that different operating systems respond differently to certain type of packets. So from response we can get information about operating system of target system. Unlike active fingerprinting- which revels the attacker's identify to the target system – passive fingerprinting enables the attacker to anonymously determine the operating systems running on the target host. Unlike active fingerprinting, in which you must actively send packets to the target system a use sniffer to log and study any response you receive, passive fingerprinting involves using a sniffer to passively analyze data sent by the target system regardless of their contents or intended destination.

It is hard to detect all things manually so a tool named Nmap is used for detecting OS, open ports, services.

2.4. Ping Sweeping

There may be time when we are not sure whether or not a particular host is connected to the Internet. In such cases we can use the ping utility, which relies on the echo request and echo reply. ICMP message too determine whether or not a remote host is alive or not.

The most important use of the ping tool is for network reconnaissance purpose. It allows attacker to automatically map out entire target network and pinpoint all alive host within a particular range of IP addresses. This process of using ping to map out the entire target network is known as ping sweeping. For this we use fping command (figure 5).

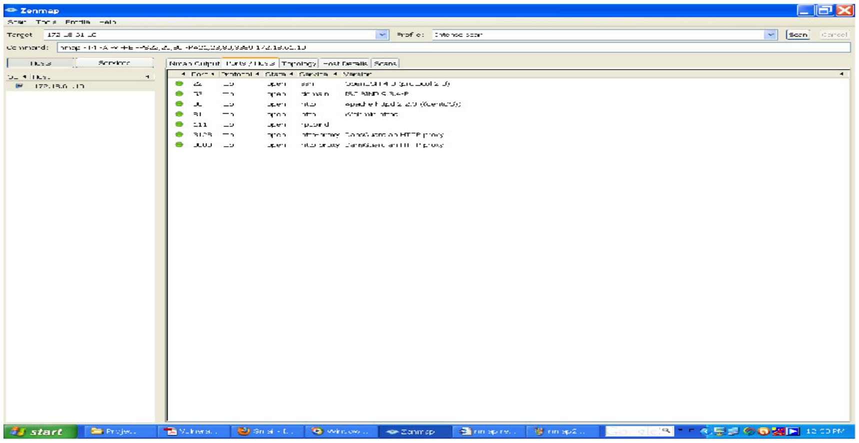


```
192.168.1.47 is unreachable
192.168.1.48 is unreachable
192.168.1.49 is unreachable
192.168.1.50 is unreachable
192.168.1.51 is unreachable
192.168.1.52 is unreachable
192.168.1.53 is unreachable
192.168.1.54 is unreachable
192.168.1.55 is unreachable
192.168.1.56 is unreachable
192.168.1.57 is unreachable
192.168.1.58 is unreachable
192.168.1.59 is unreachable
192.168.1.60 is unreachable
192.168.1.61 is unreachable
192.168.1.62 is unreachable
192.168.1.63 is unreachable
192.168.1.64 is unreachable
192.168.1.65 is unreachable
192.168.1.66 is unreachable
192.168.1.67 is unreachable
192.168.1.68 is unreachable
192.168.1.69 is unreachable
192.168.1.70 is unreachable
192.168.1.71 is unreachable
192.168.1.72 is unreachable
192.168.1.73 is unreachable
192.168.1.74 is unreachable
192.168.1.75 is unreachable
192.168.1.76 is unreachable
192.168.1.77 is unreachable
192.168.1.78 is unreachable
192.168.1.79 is unreachable
192.168.1.80 is unreachable
192.168.1.81 is unreachable
192.168.1.82 is unreachable
192.168.1.83 is unreachable
192.168.1.84 is unreachable
192.168.1.85 is unreachable
```

Figure 5: ping sweeping

2.5. Port Scanning

Port scanning is the art of scanning the target systems to obtain a list of open ports that are listening for connation. In this, we connects to various TCP and UDP ports and tries to determine which ports are in listening mode. To find out open ports we use nmap command (in figure 6)

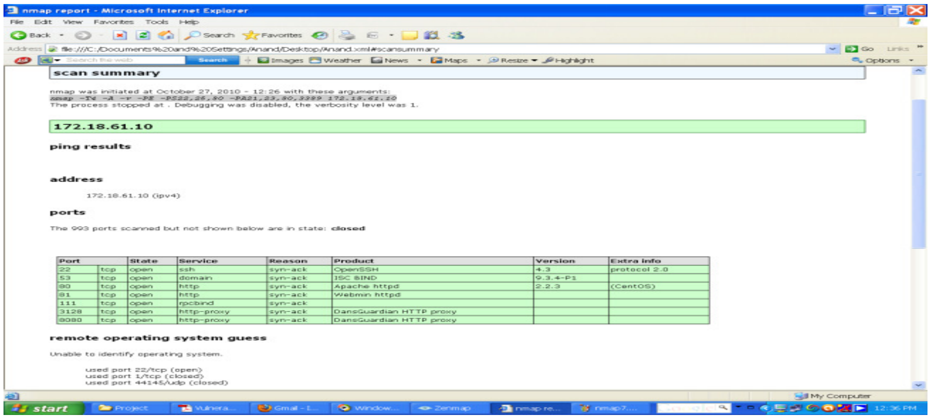


```
Target: 172.18.61.10          Profile: Intense scan
Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 172.18.61.10

Port   Protocol  State  Service     Version
22     tcp       open   ssh         OpenSSH 4.3 (protocol 2.0)
53     tcp       open   domain      ISC BIND 9.3.4-P1
80     tcp       open   http        Apache httpd 2.2.3 ((CentOS))
81     tcp       open   http        Webmin httpd
111    tcp       open   rpcbind
3128   tcp       open   http-proxy  DansGuardian HTTP proxy
8080   tcp       open   http-proxy  DansGuardian HTTP proxy
```

Figure 6: Number of open ports on target system

It is difficult to get information manually so one tool nmap is used for detection of operating system, open port, ping sweeping. So this is a report of nmap(figure 7)



scan summary

nmap was initiated at October 27, 2010 - 12:26 with these arguments:
`nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 172.18.61.10`
The process stopped at . Debugging was disabled, the verbosity level was 1.

172.18.61.10

ping results

address

172.18.61.10 (ipv4)

ports

The 993 ports scanned but not shown below are in state: **closed**

Port		State	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	4.3	protocol 2.0
53	tcp	open	domain	syn-ack	ISC BIND	9.3.4-P1	
80	tcp	open	http	syn-ack	Apache httpd	2.2.3	(CentOS)
81	tcp	open	http	syn-ack	Webmin httpd		
111	tcp	open	rpcbind	syn-ack			
3128	tcp	open	http-proxy	syn-ack	DansGuardian HTTP proxy		
8080	tcp	open	http-proxy	syn-ack	DansGuardian HTTP proxy		

remote operating system guess

Unable to identify operating system.

used port 22/tcp (open)
used port 1/tcp (closed)
used port 44145/udp (closed)

nmap report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address file:///C:/Documents%20and%20Settings/Anand/Desktop/Anand.xml#scansummary
Search Images Weather News Maps Resize Highlight
My Computer
start Project Vulnera... Gmail - I... Window... Zenmap nmap re... nmap7....

Figure 7: NMAP Report

It gives information of host (172.18.61.10) like operating system on host machine is windows. There are 7 open ports.

3. USEFULNESS OF INFORMATION FOR ATTACKER

For attacker to attack a target system above find information is very useful. In this section we are going to describe, how this information is useful for an attacker.

Table 3: Usefulness of information to an attacker

Information	Usefulness
IP address	To uniquely identify target
Operating system	To find out loopholes
Port scanning	To break target systems
Firewall	To change policies
Ping Sweeping	To find out number of systems active in network

3.1. IP address

Every computer that connects to the Internet is assigned an IP (Internet Protocol) address. This is very similar to a telephone number in many ways. If you have a DSL connection or cable modem connection your IP address stays the same and is "always on". If you have a "dial-up" account, then your IP address is dynamic (it changes each time you connect), and your ISP (Internet Service Provider) cuts you off after a certain amount of time of inactivity. It is useful to uniquely identify target system in whole world.

Dial-up accounts are less hacker friendly because your IP address changes each time you are on. This makes it impossible for the hacker to make repeat visits unless he has tricked you into loading a program on your PC that tells him when you are on-line and gives him your current IP address. "Always on" connections are just that, always connected and open for attack.

3.2. Operating system

This information is very useful during the attack phase when attacker is exploiting a loophole to infiltrate the system. Most home PCs run Windows, so hacking is easy because there are many known Window "bugs" that can be taken advantage of. Most home users have never worried about computer security.

Hackers look for commonly know system weaknesses (bugs or holes in software). The operating system, like Windows, has bugs, as do other software like browsers, such as Microsoft's Internet Explorer. They scan your open ports looking for a running program that they can take advantage of. Scanning is like a burglar who checks all the doors and windows of your house to see if any are unlocked.

3.3. Port scanning

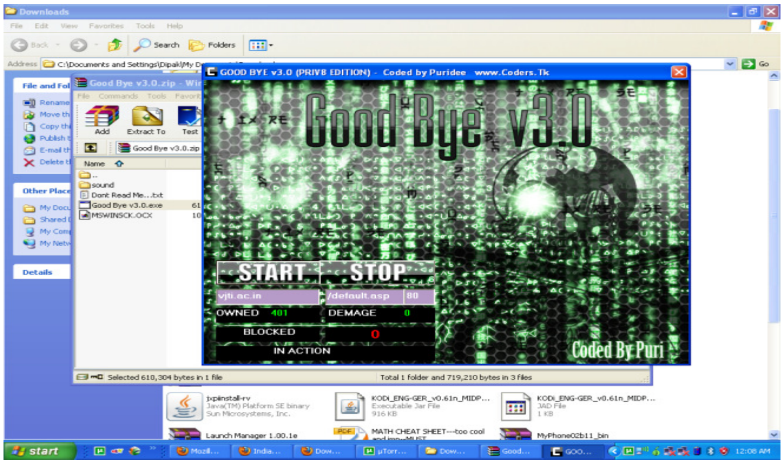
This is crucial for an attacker because it helps to determine the list of open ports on the target system, the services running on them and any vulnerability that might exist. When a port is found to be open, it means that some type of service is running on that port, and there's a chance that the attacker can exploit it for the purposes of gaining remote access to the computer system. With a proper access exploit in place, an attacker could potentially gain control of the computer system.

3.4. Firewall

A firewall is used to protect a network from Internet intruders. Packets entering a firewall are checked against an Access Control List (ACL). TCP packets sent by a source are acknowledged by acknowledgment packets. If a packet seems like an acknowledgement to a request or data from the local network, then a stateful firewall also checks whether a request for which this packet is carrying the acknowledgment was sent from the network. If there is no such request, the packet is dropped, but a stateless firewall lets packets enter the network if they seem to carry an acknowledgment for a packet. Most probably the intended receiver sends some kind of response back to the spoofed address. Again, for this process to work, the attacker should be able to see the traffic returning to the host that has the spoofed address—and the attacker generally knows how to use the returned packet to advantage.

4. TOOLS TO DO ATTACKS

By gathering information such as IP address, operating system, firewall, number of open ports and number of alive systems in a network we can perform attack with the help of tools. We can perform DDOS attack with the help of tool Good Bye V3.0 and to perform IP spoofing, we take help of TOR software with add on tor-button. With IP address we identify the target system.


GOOD BYE v3.0 (PRIV8 EDITION) - Coded by Puridee www.Coders.Tk
Good Bye v3.0
START
STOP
Coded By Puri

vjti.ac.in | /default.asp | 80
OWNED 401 | DEMAGE 0
BLOCKED 0
IN ACTION

Figure 8: Write Web site and Click on start

It is a view of software (Figure 8).

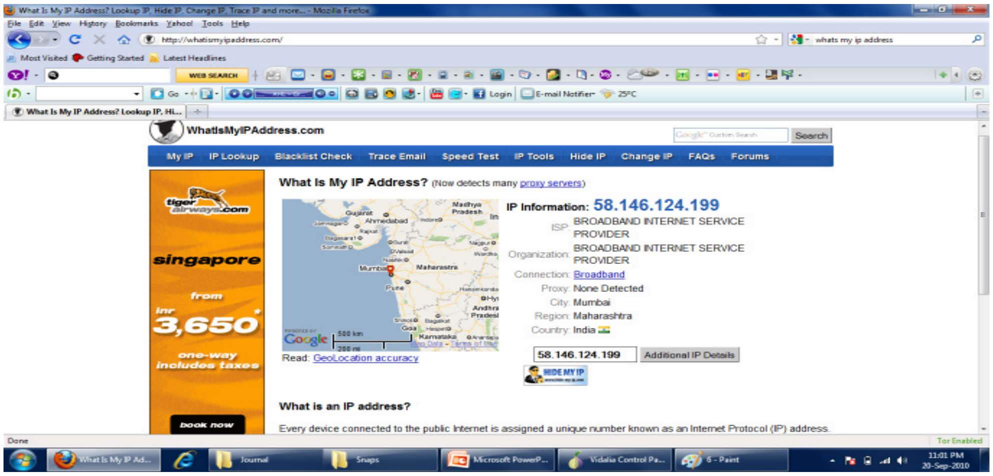
We have to write website address (such as www.vjti.ac.in) with a page (such as /default.asp), so your full address is www.vjti.ac.in/default.asp.

For **IP spoofing** we have to download TOR software with add on tor-button.

- First time tor button (at the bottom right corner) is disabled.
- After this we will enable that button.

This time information of our system is (Figure 9)

- IP address : 58.146.124.199
- ISP : Broadband Internet Service provider
- City : Mumbai
- Region : Maharashtra
- Country : India



What Is My IP Address? (Now detects many proxy servers)

IP Information: 58.146.124.199
ISP: BROADBAND INTERNET SERVICE PROVIDER
Organization: BROADBAND INTERNET SERVICE PROVIDER
Connection: Broadband
Proxy: None Detected
City: Mumbai
Region: Maharashtra
Country: India

Read: GeoLocation accuracy

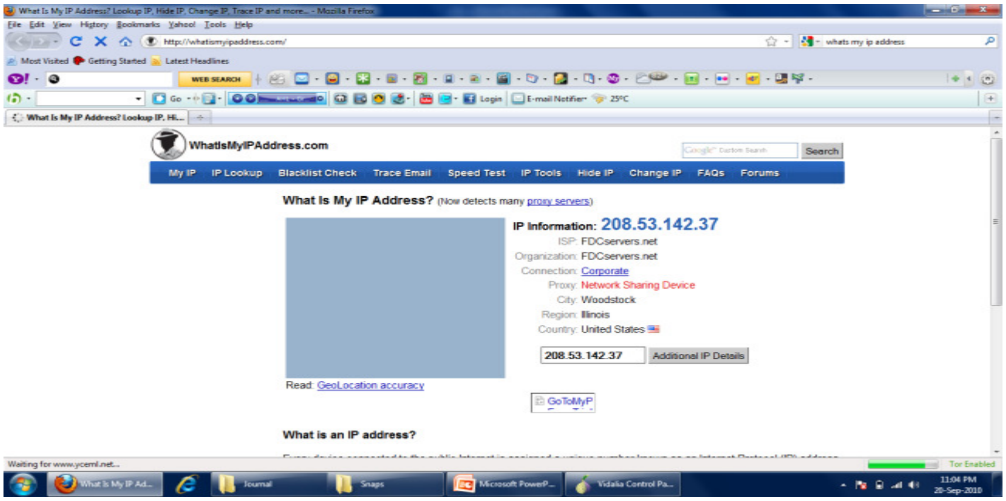
What is an IP address?

Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address.

Figure 9: IP Information (Tor Disabled)

This time we enable the tor button and color will change to green.

- And open Vidalia control panel.
- Click on new identity button.



What Is My IP Address? (Now detects many proxy servers)

IP Information: 208.53.142.37

ISP: FDCservers.net
Organization: FDCservers.net
Connection: Corporate
Proxy: Network Sharing Device
City: Woodstock
Region: Illinois
Country: United States

208.53.142.37

Read: GeoLocation accuracy

What is an IP address?

Waiting for www.yceml.net...

Figure 10: IP Information (Tor Enabled)

Now this time information of our system is(Figure 10)

- IP address : 208.53.142.37
- ISP : FDCsevers.net
- City : Woodstock
- Region : Illinios
- Country : United State

For every time it give different information.

5. PROPOSED MODEL

Defending against DDOS attack is a critical issue, in this we have to differentiate normal traffic and DDOS attack. In this aggressiveness is the factor that is important to differentiate. A true user always check what it receive but attacker don't care whether it may receive the response from the victim or not, and send too many packets to victim or increase the rate. High rate is different from aggressiveness, some time true user also send packet in high rate.

To detect IP spoofing Hop count value is key factor. Because if there is IP spoofing then Hop count value changes, if there is change in value greater then threshold value (decide by user) then we can say that there is IP spoofing attack take place.

If both attacks take place at same time then it is very difficult to protect our system from this so for this we proposed a model(Figure 11). In this model when a packet arrive then first we check that is it new packet or not? If packet comes first time then first we check flow count (FC), set by user. If flow count is greater then FC then drop that packet otherwise increase FC by one and create IP2HC (IP to hop count table) and send acknowledgment to sender. IP2HC table is a simple table that has source IP address and hop cont value.

If old packet come then check for this IP address how much time it passes test if pass test value is less than P (set by user) than it goes for checking fail test. It is important to set value of P, if we set value of P very low then it doesn't help us, because it always go to check fail test. In next step fail test of that IP is check if fail test is greater than F (set by user) then drop that packet. If less than then check rate, current rate should be less than half of previous rate and increment pass test by one otherwise increment fail test by one and drop that packet. After increment value of pass test and if pass test is greater than P then we go to next step and find final TTL value(TTL_I), thane find Final TTL value (TTL_F) and calculate new hop count (HC_N) by taking difference of TTL_F , TTL_I. Fetch IP address from packet and previous hope count HP_P. If difference of HC_N and HC_P is greater than threshold value then drop that packet otherwise update hope count value for that source IP with average of HC_N and HC_P.

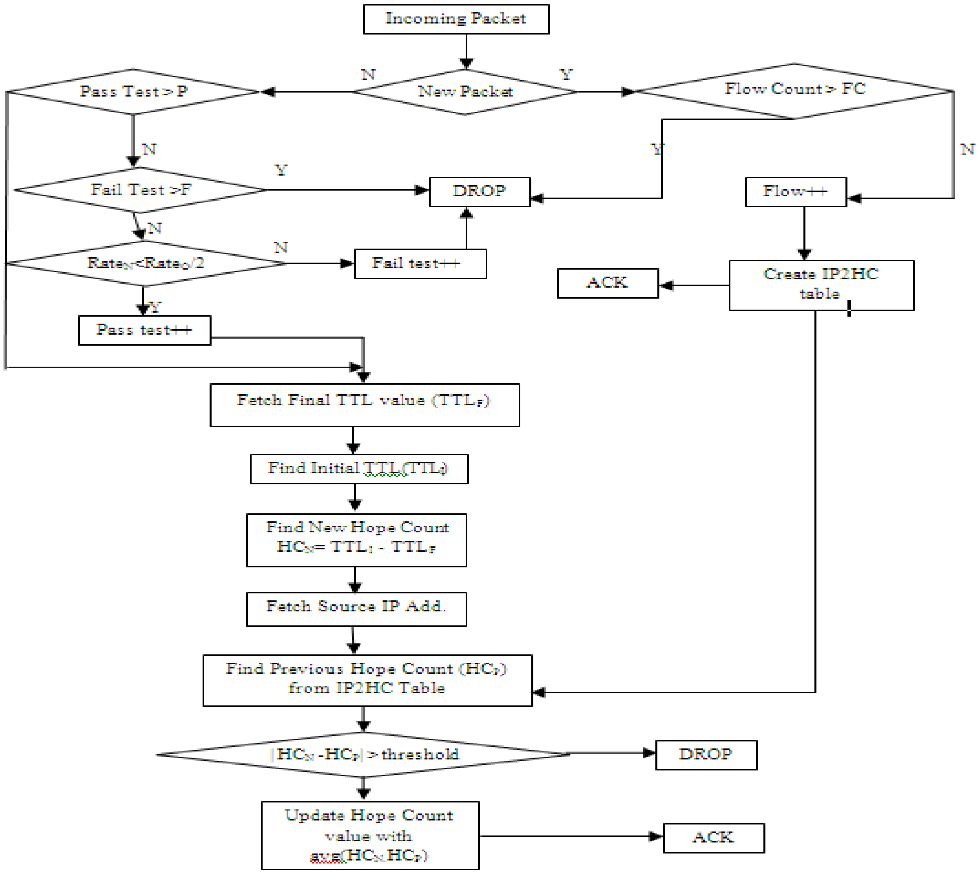


Figure 11: Proposed Solution

6. CONCLUSION

In this paper we have discussed about DDOS and IP spoofing attacks. Both attacks are very dangerous and most popular; it is very difficult to detect these attacks. When DDOS attack come together with IP spoofing then it is more difficult to detect, and more dangerous. We have gathered the information such as IP address, operating system, firewall, number if alive systems in network and number of open ports to do attacks. This information is useful to do attack with the help of tools. Lastly weaknesses were hardened with the help of proposed model.

7. REFERENCES

[1] Zhiqiang Gao, Nirwan Ansari,” Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests” in IEEE and ISBN no is 1089-7798/06.

[2] Amey Shevtekar and Nirwan Ansari,” Is It Congestion or a DDoS Attack?” in IEEE and ISBN no. is 1089-7798/09.

[3] Greg Goth,” The Politics of DDoS Attacks “ in IEEE and art no. 0708-o8003 .

[4] RAMAMOHANARAO,” Survey of Net work-Based Defense Mechanisms Countering the DoS and DDoS Problems” in ACM 0360-0300/2007/04-ART3.

[5] Stefan Savage, David Wetherall, Anna Karlin, and Tom A] TAO PENG, CHRISTOPHER LECKIE, and KOTAGIRI nderson.” Network Support for IP Traceback” in IEEE 1063–6692/01

[6] Indrajeet B. Mopari, S. G. Pukale,M. L. Dhore,” in ACM 978-1-60558-351-8 *ICAC3’09*