Available online at http://www.journalcra.com

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

International Journal of Current Research
Vol. 5, Issue, 01, pp.006-013, January, 2013

ISSN: 0975-833X

RESEARCH ARTICLE

Attcack and Saving Network from Attack

***Luaay Abdulwahed**

College of nursing, Basra University, Iraq **Corresponding author:* Loea1965@yahoo.com, luaay.shihab@uobasrah.edu.iq

ARTICLE INFO

Article History:
Received 25th October, 2012
Received in revised form
28th November, 2012
Accepted 7th December, 2012
Published online 16th January, 2013

Key words:

DOS/IP/ICMP/TCP/UDP/
DNS/HTTP

ABSTRACT

This paper takes a keen look in network security and network security goals, why computers are insecure and type Of attack, how to improve network security . Securing your network and practical's what is Quota.

INTRODUCTION

Network security comprises the measures a company takes to protect its computer system, and it is a prime concern for every company that uses computers. Compromised network security means a hacker or competitor may gain access to critical or sensitive data, possibly resulting in data loss, or even complete destruction of the system .

Network Security Goals

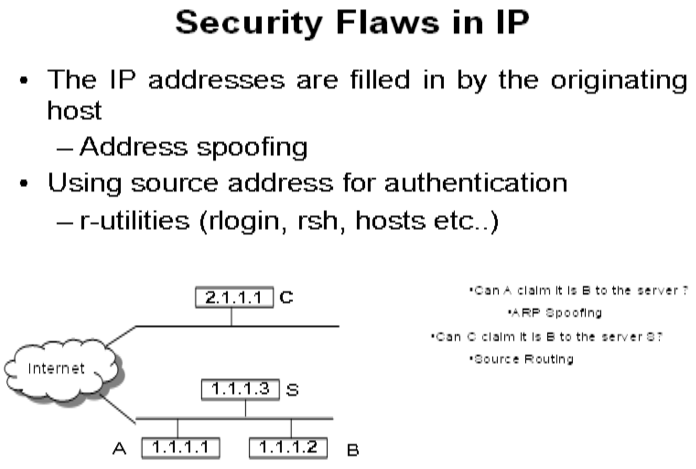
- Confidentiality: only sender, intended receiver should "understand" message contents sender encrypts message receiver decrypts message Privacy: hide `who is doing what with whom
- Authentication: sender, receiver want to conform identity of each other
- Integrity: sender, receiver want to ensure messages are not altered (in transit, or afterwards) without detection
- Access and Availability: services must be accessible and available to users Network Security

Why Computers are Insecure ?

Most PCs use insecure Ross

- Most designed for `home` - security not a goal
- Others support separation between users
- Few/none restrict capabilities of applications
- Malicious / vulnerable / buggy app can harm all!!

PCs run buggy, vulnerable, even malicious code Many sources (libraries, shareware, …)
Limited awareness & tools.
Limited product liability and consequent damages
Most computers don't fix known vulnerabilities



Security Flaws in IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, hosts etc..)

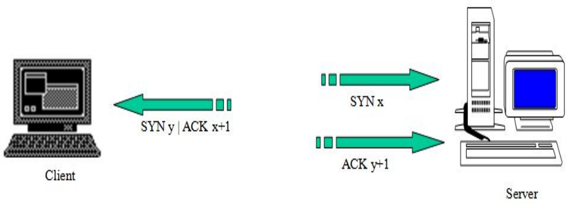
2.1.1.1 C
Internet
1.1.1.3 S
A 1.1.1.1
1.1.1.2 B

•Can A claim it is B to the server ?
•ARP Spoofing
•Can C claim it is B to the server S?
•Source Routing

Routing Attacks

- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Black hole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP
  - ASes can announce arbitrary prefix
  - ASes can alter path

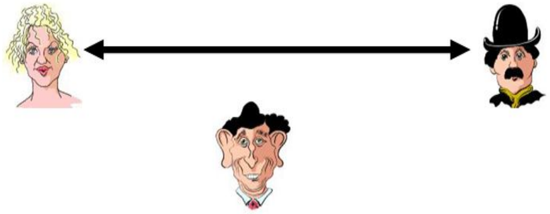
TCP Attacks



Issues?
- Server needs to keep waiting for ACK y+1
- Server recognizes Client based on IP address/port and y+1

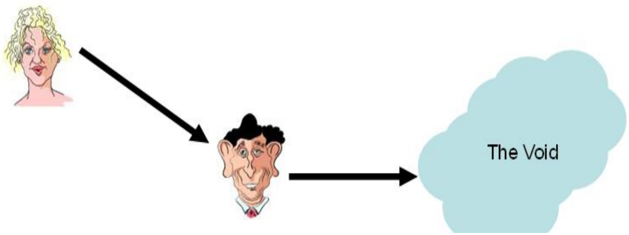
TCP Attacks

- Nikks and Luaay have an established TCP connection



TCP Attacks

- First, Mr. Danger Ears must drop all of Nikks packets since they must not be delivered to Bob (why?)



TCP Attacks

Why are these types of TCP attacks so dangerous?

Web server

Trusting web client

Malicious user

TCP Layer Attacks

- **TCP Session Hijack**
  - When is a TCP packet valid?
    - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it
      - Many earlier systems had predictable ISN
  - Inject arbitrary data to the connection
- **TCP Session Poisoning**
  - Send RST packet
    - Will tear down connection
  - Do you have to guess the exact sequence number?
    - Anywhere in window is fine
    - For 64k window it takes 64k packets to reset
    - About 15 seconds for a T1

Attacks on UDP

- Fields in first 64 bits: Source Port, Destination Port, Length, Checksum Bits 65-128: Data payload
- Dest. Port: Decrypted packets delivered to X_B.
- Length: Packets can be truncated.
- Checksum can be fixed directly
- With a 128-bit cipher, the first 64 bits of the payload can be modified.

IV Attacks on L2TP

Layer 2 Tunneling Protocol (L2TP):
- Used to tunnel PPP connections over a wide area network.
- L2TP data packets encapsulated in UDP
- Typically uses IPsec ESP for encryption

IV attack on L2TP with IPsec ESP:
- 128-bit IV reaches the first 64 bits of L2TP packet
- contains Length, Tunnel ID, Call ID
- Call ID attack: Decrypted packet can be delivered to attacker's connection. (similar to attack on TCP/UDP Destination Port)

– Attacks On Application Layer

Applications don't authenticate properly

Authentication information in clear
- FTP, Telnet, POP

DNS insecurity

Types of attacks

- Denial of Service (DoS) Attacks
- □□ Website Defacement
- □□ Viruses and Worms
- □□ Data sniffing and Spoofing
- □□ Unauthorized Access
- □□ Malicious Code and Trojans
- □□ Port-scanning and Probing
- □□ Wireless Attacks

Denial O f Service (Clogging) Attack

- Denial Of Service (Clogging) Attack Attacker tries to exhaust resources of host /server / router / user
- Resources include:-
- Computations (CPU time) Storage
  (e.g. for state of requests/connections)
- Open TCP connections
- Limited (10s to several thousand connections -depending on hardware, operating system)
- So server `never` keeps open connections !Always request-response (and server closes connection, no state)
- SYN flooding DOS attack: attacker sends` SY N` flow (open connection); server waits…Network Security

SYN flooding DOS (clogging) Attack

- Recall T CP connection setup process
- Attacker sends many SY N requests (using different spoofed client IP addresses), no ACK
- Uses up server's capacity for open connections
- Possible solution: request must contain `cookie' (next)

Attacks Through The Net

- **Eavesdropping**
- **Port scanning (probing for weaknesses)**
- **Spoofing—**
  Fake e-mail
  – Using a fake IP address
- **Denial of Service (DoS)–**
  Shut down the target host via a critical fault–
  Also available in distributed format to simply overload a target
  Message replay
- **Connection capture (TCP)**

Port-scanning

- – Technique that identifies vulnerable network ports or services (i.e. TELNET, FTP, E-mail, Web, etc)
- – Works by identifying as many targets as possible and tracking the ones that are receptive
- – Scanning software is free and commonly accessible via the web

(Spoofing)

- IP spoofing **-** An attacker may fake their IP address so the receiver thinks it is sent from a location that it is not actually from. There are various forms and results to this attack.
- The attack may be directed to a specific computer addressed as though it is from that same computer. This may make the computer think that it is talking to itself. This may cause some

operating systems such as Windows to crash or lock up

Man in the middle attack -

- Session hijacking – An attacker may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it, and use IP spoofing to claim to be the client who was just authenticated and steal the session. This attack can be prevented if the two legitimate systems share a secret which is checked periodically during the session.
-

(DNS POISONING)

- - This is an attack where DNS information is falsified. This attack can succeed under the right conditions, but may not be real practical as an attack form. The attacker will send incorrect DNS information which can cause traffic to be diverted. The DNS information can be falsified since name servers do not verify the source of a DNS reply. When a DNS request is sent, an attacker can send a false DNS reply with additional bogus information which the requesting DNS server may cache. This attack can be used to divert users from a correct web server such as a bank and capture information from customers when they attempt to logon.

Some DoS Attacks

- –Ping broadcast : A ping request packet is sent to a broadcast network address where there are many hosts. The source address is shown in the packet to be the IP address of the computer to be attacked. If the router to the network passes the ping broadcast, all computers on the network will respond with a ping reply to the attacked system. The attacked system will be flooded with ping responses which will cause it to be unable to operate on the network for some time, and may even cause it to lock up. The attacked computer may be on someone else's network. One countermeasure to this attack is to block incoming traffic that is sent to a broadcast address.
- Ping of death – An oversized ICMP datagram can crash IP devices that were made before 1996.
- Smurf – An attack where a ping request is sent to a broadcast network address with the sending address spoofed so many ping replies will come back to the victim and overload the ability of the victim to process the replies.
- Teardrop – a normal packet is sent. A second packet is sent which has a fragmentation offset claiming to be inside the first fragment. This second fragment is too small to even extend outside the first fragment. This may cause an unexpected error condition to occur on the victim host which can cause a buffer overflow and possible system crash on many operating systems.

Wireless Attacks

- Wireless Equivalent Privacy (WEP) protocol cannot be trusted for security
- Attackers can easily eavesdrop or spoof wireless traffic
- Hackers external to your building may be able to intercept and view all of your wireless traffic, despite encryption
- Hacker tools free and easily accessible via the web: AirSnort, WEPCrack.

How to improve network security

- General awareness of Network Security among users
- Upgrading the skill of the system and network administrators
- Sharing of network security information, knowledge and experience amongst system and network administrators

Countermeasure

- Personnel Security Policy and Procedures
- Training and Awareness
- Physical Security
- Dedicated Management Technology
- Firewalls
- Intrusion Detection
- Virus Protection
- Authentication and Authorization
- Encryption
- Auditing and Assessment (Third Party)
- Data and Information Backup

SSH

SSH can be used for secured Command and Control sessions to routers.

- Full SSH has three components
- a terminal session with a secure transport
- the ability to handle "r-commands" similar to rsh
- the ability to "forward" other TCP-based protocols

SSH Authentication

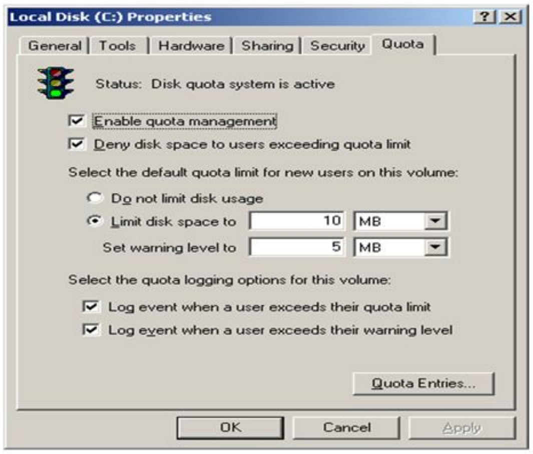
- There are two levels of
- Authentication required for an SSH session
- Host (or 'device') Authentication
- User Authentication

What is Quota

- To select other options as desired: enable disk quotas for the users, log on as an administrator, right click on the drive you want to limit, and select the quota tab. Check **Enable quota management**, and select other options as desired:

Quota Management

- Open properties of any drive on which you want to add quota limit.
- Shown in figure 1.1



Status: Disk quota system is active

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 10 MB

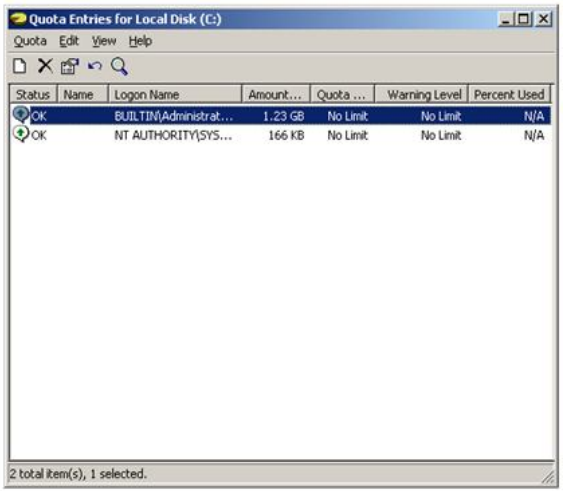
Set warning level to 5 MB

Select the quota logging options for this volume:

☑ Log event when a user exceeds their quota limit

☑ Log event when a user exceeds their warning level

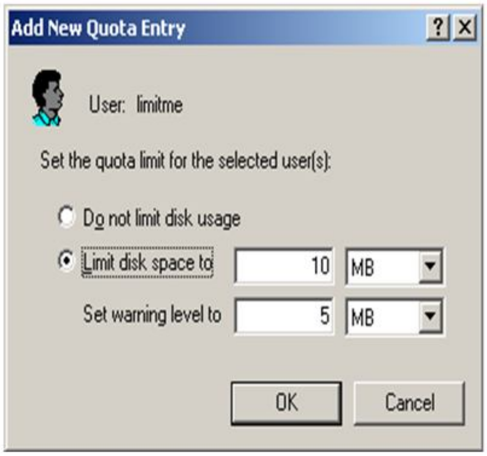
- Then select Quota tab and select new entry to add quota limit.
- Shown in figure 1.2



Status	Name	Logon Name	Amount...	Quota ...	Warning Level	Percent Used
OK		BUILTIN\Administrat...	1.23 GB	No Limit	No Limit	N/A
OK		NT AUTHORITY\SYS...	166 KB	No Limit	No Limit	N/A

2 total item(s), 1 selected.

- Then select space which you want to provide a user for the use..
- Shown in figure 1.3



Add New Quota Entry

User: limitme

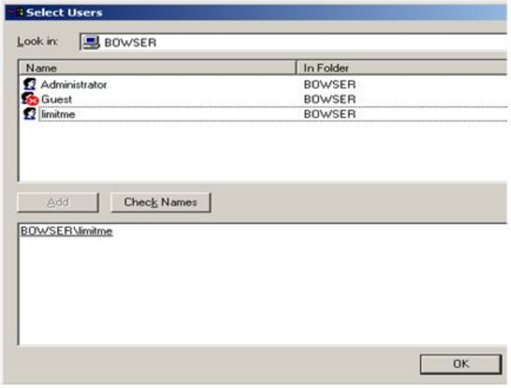
Set the quota limit for the selected user(s):

○ Do not limit disk usage

● Limit disk space to 10 MB

Set warning level to 5 MB

- Then select user on which you want to add quota limit.
- Shown In figure 1.4



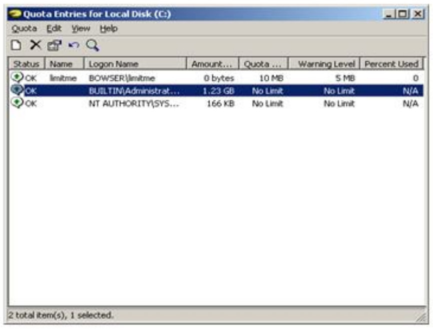
Select Users

Look in: BOWSER

Name	In Folder
Administrator	BOWSER
Guest	BOWSER
limitme	BOWSER

BOWSER\limitme

- After selecting user you will find that your user is in the list on which you r applying quota limit. And then click finish.
- Shown in figure 1.5

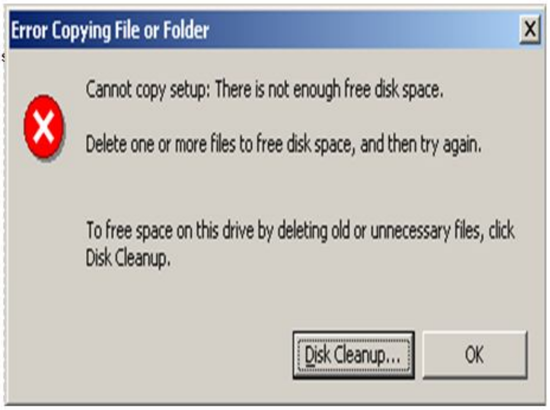


Quota Entries for Local Disk (C:)

Status	Name	Logon Name	Amount...	Quota ...	Warning Level	Percent Used
OK	limitme	BOWSER\limitme	0 bytes	10 MB	5 MB	0
OK		BUILTIN\Administrat...	1.23 GB	No Limit	No Limit	N/A
OK		NT AUTHORITY\SYS...	166 KB	No Limit	No Limit	N/A

2 total item(s), 1 selected.

- After applying quota limit a user will find thi error log.
- Shown in figure 1.6



Error Copying File or Folder

Cannot copy setup: There is not enough free disk space.

Delete one or more files to free disk space, and then try again.

To free space on this drive by deleting old or unnecessary files, click Disk Cleanup.

REFERENCES

Advanced wireless networks . second edition Savo Glisic ,Beatriz Lorenzo (2009).

CCNA sixth edition (Cisco certified network associate)by Todd Lammle.

Communication networks .Sharma hekmet (2005).

Concept of network second edition by institute of hardware technology (2005).

Internet working with tcp / ip fifth edition –Douglas e. comer (2006)

Network configuration first edition by institute of hardware technology (2003).

Security+certification second edition by Microsoft corporation

Wireless networking in the developing world . Second edition, hacker friendly, December (2007).

****