Subverting Networks

Parul Khanna

mail@parulkhanna.info

About Me :

- CTO & President Third Eye Ethical Hackers Society®.
- Sr.Cellular Technology Evangelist & Trainer @ Secugenius Security Solutions .
- Brand Ambassador at INGHC,USA.
- Security Lead at Third Eye Intelligence Beaurau,Hyd.
- CSA @ Progress Solutions Inc. Tampa,Florida (USA).
- Security Architect @ iTnukes.com ,UK
- General Secretary @ Cyber Security Anti Hacking Organisation of India.

Overview

- What is security?
- Why do we need security?
- Who is vulnerable?
- Common security attacks and countermeasures
  - Firewalls & Intrusion Detection Systems
  - Denial of Service Attacks
  - Packet Sniffing
  - Social Engg.

What is Security ?

- As Per Dictionary :

*The state of being free from danger or threat

- having systems in place beforehand which prevent attacks before they begin .
- Something that gives or assures safety, as:
  - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
  - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
  - 3. Measures adopted

-This includes contingency plans for what to do when attackers strike, keeping up with the latest CERT advisories,

-hiring network security consultants to find insecurities in your network, etc.

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Protect Portfolio Information of Admin's/ Users/Subscribers.
- Provide authentication and access control for resources
  - Ex: AFS

Who is vulnerable?

- Financial institutions and banks
- Social Networking Websites
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- Regular Internet Users
- **ANYONE ON THE NETWORK……**

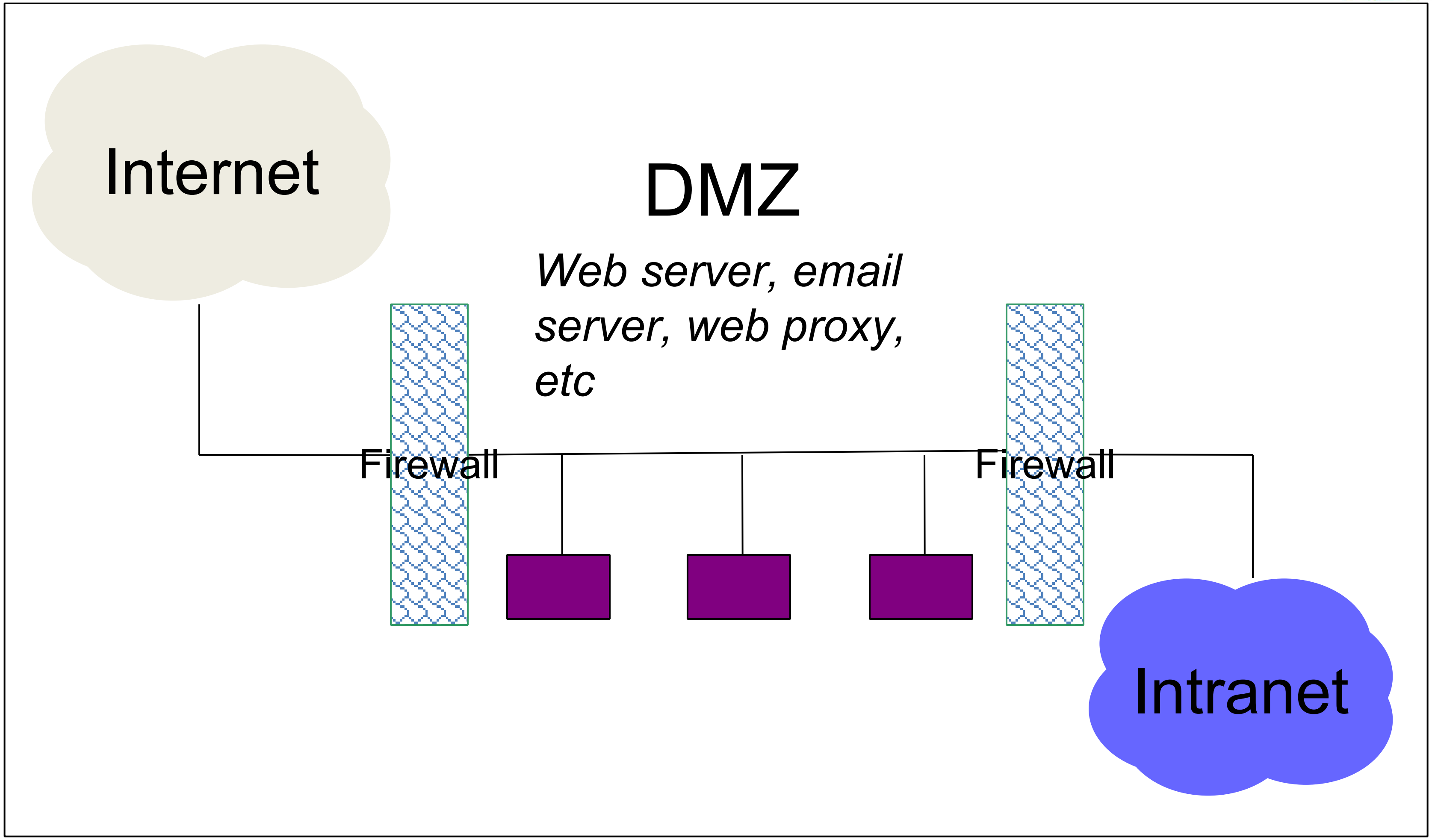
Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social Engg.
  - Awareness

Firewalls

- Basic problem – many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators

Firewalls


Internet
DMZ
Web server, email server, web proxy, etc
Firewall
Firewall
Intranet

Intrusion Detection

- Used to monitor for “suspicious activity” on a network
  - – Can protect against known software exploits, like buffer overflows
- Open Source IDS: Snort, www.snort.org

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, “sdfo839f” is a good password
    - That is not my andrew password
    - Please don’t try it either

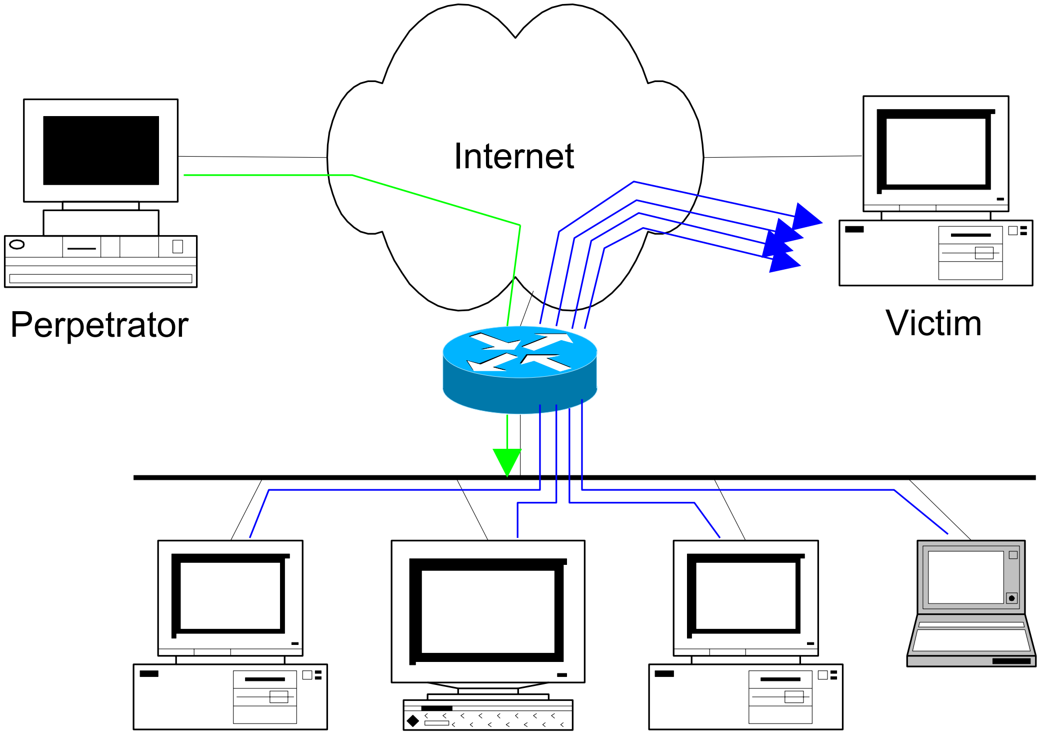
Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks
  - Mini Case Study: Code-Red

Denial of Service

🟩 ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

🟦 ICMP echo reply



Denial of Service

- How can we protect ourselves?
  - Ingress filtering
    - If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it
    - RFC 2267 has more information about this
  - Stay on top of CERT advisories and the latest security patches
    - A fix for the IIS buffer overflow was released **sixteen days before** CodeRed had been deployed!

Packet Sniffing

- Recall how Ethernet works …
- When someone wants to send a packet to some else …
- They put the bits on the wire with the destination MAC address …
- And remember that other hosts are listening on the wire to detect for collisions …
- It couldn’t get any easier to figure out what data is being transmitted over the network!

Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium

Packet Sniffing

- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
  - Passwords are the most popular

Packet Sniffing

- How can we protect ourselves?
- SSH, not Telnet
  - Many people at CMU still use Telnet and send their password in the clear (use PuTTY instead!)
  - Now that I have told you this, please do not exploit this information
  - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
  - Especially when making purchases with credit cards!
- SFTP, not FTP
  - Unless you ***really*** don't care about the password or data
  - Can also use KerbFTP (download from MyAndrew)
- IPSec
  - Provides network-layer confidentiality

Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the "harmed" stage, unless they have been specially trained
    - Think government here…

Social Problems

- Fun Example :
  - “Hi, I’m a VODAFONE rep, I’m stuck on a pole. I need you to punch a bunch of buttons for me”

Social Problems

- There aren’t always solutions to all of these problems
  - Humans will continue to be tricked into giving out information they shouldn’t
  - Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
- So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information
  - But, this solution is still not perfect

Contact :

Parul Khanna

Email : mail@parulkhanna.info

Blog : www.parulkhanna.info

Become a Fan on Facebook www.facebook.com/parulkhannaofficial

Find me on facebook www.facebook.com/connectparul