Network Security

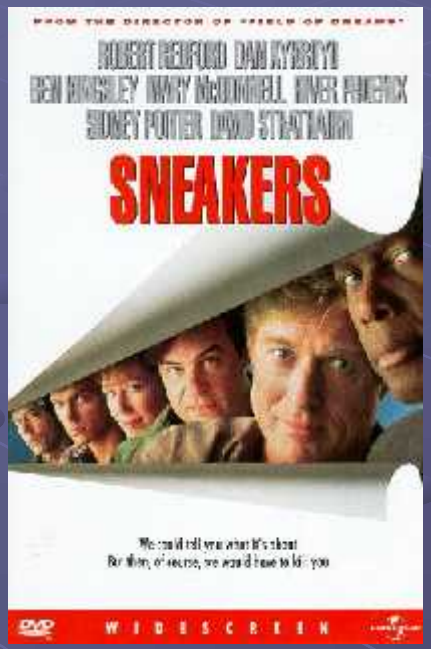
System Security

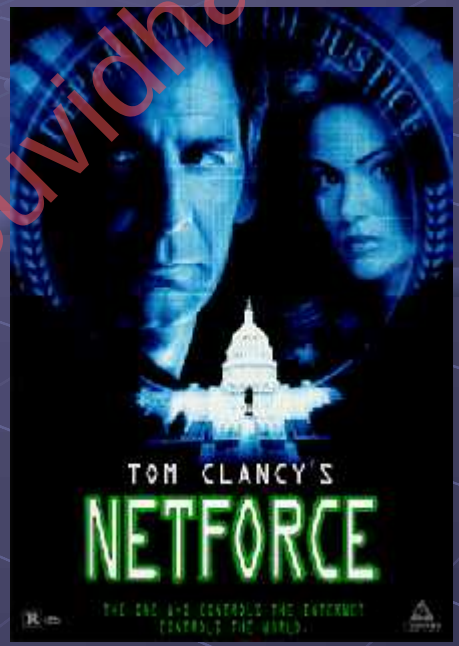
- Security is one of the most critical aspects of any network
- A computer network is only as strong as its weakest link
- Computer security has become more important than ever

Hacker vs. Cracker

- We hear of malicious individuals breaking into corporate and government computer systems around the world.

- The media calls these people hackers. This description ***is not*** entirely accurate.





Hacker vs. Cracker

Hacker - Within the subculture of computer hobbyists and software enthusiasts, the term “Hacker” usually refers to a particular kind of **programmer**.

- Someone who programs creatively
- Someone who programs for pure enjoyment (most programmers who work on Linux are hackers in this case)

Cracker - Is someone who **breaks into computers**, often to do something malicious such as steal credit card information.

- Many types, ranging from professional computer criminals to the hobbyist who breaks into computers for the thrill
- Teenage pseudo crackers do not have the knowledge of their true cracker counterparts, but have access to their tools to automate breaking into a system.
- Using the programs and scripts of truly talented crackers youngsters can break into a system without really knowing how they did it
- Those who depend on a tool or script to break into a system are often referred to as a “Scriptkiddies”

Important Steps to Security

- Password Protection
- Protecting the network by filtering Network Access and Traffic (i.e. ***Firewall***)
- Running Security Audits
- Examine and monitor log files
- Make use of Intrusion Detection tools
- Use common sense: avoid dumpster divers and social engineers

Password Protection

Passwords are the most fundamental security tool of any modern operating system and the most commonly attacked feature.

Don’ts of choosing a password:

- Don’t use a variation of your login name or full name, this will still be an easily guessed password.
- Don’t use a dictionary word, even if you add numbers or punctuation to it.
- Do not use any contiguous line of letters or numbers on the keyboard (such as “qwerty” or “asdfg”)

Do’s of choosing a password:

- A good way to choose a strong password is to take the first letter from each word of an easily remembered sentence. Some examples are listed below:

Password	How to Remember it
Mrci7yo!	My rusty car is 7 years old!
2emBp1ib	Two elephants make BAD pets, 1 is better
ItMc?Gib	Is that MY coat? Give it back

System Admin Tips for passwords

- Change or force users to change passwords periodically
- Encrypt password files within your server or database
- Test your passwords with the same tools that crackers use such as a utility called “Crack”

System Security

Filter Network Access

Many network services can run on your network so as a system administrator you should be aware of them and limit access to the appropriate users.

Provide Administrators a secure access method

Do not attempt to use administration tools that do not support encryption. A better policy employs the use tools like SSH which allows remote access through a shell with a 128 bit encrypted connection.

Firewalls

A firewall is a computer, hardware, or even a piece of software that sits between your network and the Internet, the firewall attempts to regulate and control the flow of information preventing an array of potential attacks.

A firewall can use either of the following methods to filter the information:

Packet filtering:- It analyzes the data stored in the incoming & outgoing packets.

Proxy Service:- The information is received in firewall & sent to the proxy server. The information is not directly sent to the requester.

IP address blocking:- The data from a particular IP address or domain name can be very easily blocked by a firewall.

Protocol blocking:- The firewall can be set to disallow a particular protocol service to a particular user or a group of user.

Port blocking:- Generally http & ftp services are available through port 80 & port 21 respectively. The firewall can be used to block a particular block.

System Security

Running Security Audits

Design a routine or make use of tools that will scan computer systems for bad configuration files, altered programs, and other potential security problems on a regular basis.

Examine and Monitor Log Files

Preparing your system for an attack is only part of the battle. You must also recognize an attack when it is occurring. Monitoring log files is part of recognizing an attack. You should monitor at least the following categories of log files:

- boot Log
- running services (i.e. HTTPD, FTP, SMTP, DHCP, …)
- log files with log-in attempts
- any general system logs

System Security

Make use of Intrusion Detection Systems

As an administrator there will be times when you are responsible for monitoring 1000's of lines of log files for multiple services. This is no doubt a daunting task. Intrusion detection systems will monitor and log all strange connection attempts and send a quick email out to administrators.

Use Common Sense

There are many forms of attacks and there are many crackers trying to use them. One of the most common forms of attack is through simple human error. One cracker may call and pretend to be a computer repair man and request that a secretary lend him a password, while another may simply sift through the trash emptied at the end of the day to salvage potentially powerful network information.

Assignment

- Why network security plays an important role ?