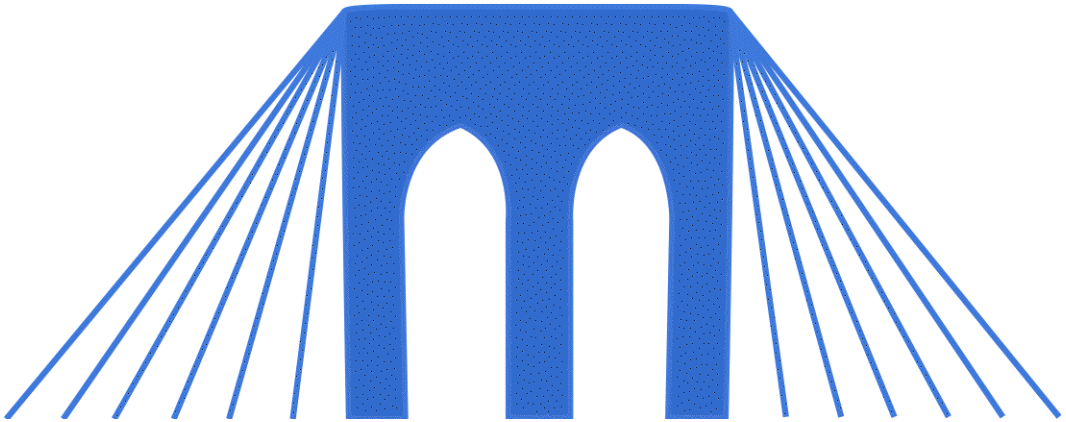
Bridges To Computing



General Information:

- This document was created for use in the "Bridges to Computing" project of Brooklyn College.
- You are invited and encouraged to use this presentation to promote computer science education in the U.S. and around the world.
- For more information about the Bridges Program, please visit our website at: http://bridges.brooklyn.cuny.edu/

Disclaimers:

- **IMAGES**: All images in this presentation were created by our Bridges to Computing staff or were found online through open access media sites and are used under the Creative Commons Attribution-Share Alike 3.0 License. If you believe an image in this presentation is in fact copyrighted material, never intended for creative commons use, please contact us at http://bridges.brooklyn.cuny.edu/ so that we can remove it from this presentation.
- **LINKS**: This document may include links to sites and documents outside of the "Bridges to Computing" domain. The Bridges Program cannot be held responsible for the content of 3rd party sources and sites.

Network Security

LECTURE 2

M. MEYER
BRIDGES TO COMPUTING
BROOKLYN COLLEGE
SPRING 2011

White hats = good guys

In this lecture we will concentrate on the problems faced by "white hat" hackers. That is, we will examine what a network security specialist needs to be aware of in order to prevent malicious theft of information from his/her company.

Setup: Alice and Bob work at two geographically separate sites. They routinely exchange, via the Internet, a file that is of very high value to a 3rd party Carol (or Charlie).

Question(s): How do **you**, as a computer security specialist (white hat) protect that file from illegal access? How might Carol (Charlie) go about stealing the file?

5 problems EVERY network security specialist should address.

1. Bribery and Blackmail
2. Physical Security
3. Eavesdropping
4. Internal system/network attack
5. External system/network attack

(1) Bribery and Blackmail

Question: What's the **easiest** way for Carol to get the file?

Answer: Get someone who has access to make her a copy.

- How much is the file worth?
- Will Alice of Bob sell the file for some fraction of its value?
- Can Alice or Bob be threated into handing over the file.
- Who else besides Alice and Bob has direct access? Can they be bribed or blackmailed?

We have had several cases of nurses (and other staff) selling the personal information of patients (including babies).

(2) Physical Security

Question: Where are copies of the secret file located?

Answer: Bob and Alice's machines, but also the main file server, any/all backup servers and tapes and every machine that handles the file when it is emailed.

- Who can physically access these machines/locations?
- Do Alice and/or Bob leave their password lying around?
- Are backup tapes stored in a secure location?
- Is the file ALWAYS stored encrypted?

(3) Eavesdropping

Question: When, where and how is the file transferred?

Answer: The file is emailed (Internet) and is also sent over the local networks at Alice and Bob's companies. Alice uses a wireless network in her office!

- Do the local networks used by Alice and Bob use SMART routers and not dumb hubs?
- Get rid of Alice's wireless network (if not possible use most advanced security available).
- Is the file ALWAYS stored/transferred encrypted?

(4) Internal system/network attack

Question: How secure are ALL internal machines?

Answer: All the machines have access to the Internet, and also run an antivirus program.

- Do all machines require logon (NO GUESTS)?
- Are all machine OS's (& antivirus) kept up to date?
- Is the network protected from unauthorized access (MAC address blocking, and limited patch panel)?
- Have users been educated on basic network security?
- Are local traffic packet records kept?
- Are machines running ONLY approved software?

(5) External system/network attack

Question: What machines can access the Internet?

Answer: ALL machines are hooked up to the Internet.

- Do all machines really need Internet access?
- Is their a firewall in place to protect networked machines (from remote port scanning).
- Are IP and DNS filters active on the firewall?
- Are servers (email, web) in a DMZ?
- Are external and DMZ traffic packet records kept?
- Is someone actively testing your security?

Conducting an AUTHORIZED external attack

1. Locating externally accessible routers and machines.
   - Searching WHOIS records.
   - Examining email headers.
   - Simple DNS requests (nslookup).
   - Ping sweeps (nmap).
   - Topology scans (traceroute, nmap)
2. Looking for weaknesses on accessible machines.
   - OS fingerprinting (nmap and other tools).
   - Port scanning (nmap and other tools).
   - Server architecture layout (based on topology and ports)

Conducting an AUTHORIZED external attack (cont)

3. Research/Write an exploit.
   - Visit ******* or ********* or ******** (or any number of other hacker sites) and look for known exploits that can be used to target machines running the OS and applications that your target machines are running – script kiddie option.
   - Using a packet creation tool (like ******* or *****) attempt to create your own exploit:
     1. Buffer overflow attack.
     2. SQL injection attack.
4. See if your own attack was detected.

Practicing at home

- It used to be difficult to practice network intrusion/detection without an actual network.
- Virtualbox is a free tool from SUN that allows you to run multiple “virtual machines” on one computer.
- DVL (d*** vulnerable linux) is a free linux based OS that comes with dozens of flawed applications already running (it can be run from a cd).
- Backtrack is a network security CD that contains all of the tools you would need to conduct an attack against a DVL machine.

The End