Lecture 7: The Kevin Mitnick attack

Who was Kevin Mitnick?

- He was an uber hacker
- Broke into organizations such as DEC, PacBell, USC, FBI, NEC, SUN, Fujitsu, Pentagon, Novell, Motorola, Nokia
- He was a binge hacker; he couldn’t control himself from hacking
- He never stole or profited from any information he hacked into
- 90% - social engineering; had a way of convincing other people to get personal information from them.
- 10% - technical wizardry

Exploits

1. Found PacBell manuals in dumpster; used the information in the manual to make free long distance phone calls
2. SCC – wiretapping system; but made clicking noises. There was another alternate system called SAS. So Mitnick called PacBell pretending to be an employee & had them read out copyright & publisher info on manual. Then he called SAS designer pretending to be from PacBell & had them fax a copy of SAS manual.
3. Social engineering of relatives
4. Called DMV while pretending to be from FBI; got them to give out records & photos.
5. Called local CO pretending to be from PacBell Security. Asked for monitor #. Then called PacBell Security pretending to be from CO. Found out he was being wiretapped.
6. Cell phones – two numbers – MIN (Mobile ID #) & ESN (Electronic Serial #); he was able to hack and clone cell phones to make free calls.

7. Scanners – was used to track cell phones within the proximity an area.

8. Almost got caught when a DMV rep. reported him to the FBI. But he physically outran the FBI at a Kinko’s (he was there to collect a DMV fax); went underground for a number of years.

9. The start of his downfall came when he wanted Oki cell phone source code; to do so he needed it from Tsutomu Shimomura’s computer. So he picked Christmas ‘95 to hack into the system and finished in a matter of a couple of minutes. This got Shimomura upset; Shimomura made a vow to catch him by aiding the FBI in their investigation. This was the turning point.

How the Shimomura computer hack was made:

1. Inputted “125.126.127.128; finger” in form that was set up by Shimomura on his webserver to run remote traceroutes and pings; “finger” checks to see if anyone is on. The string was allowed because the IP box allowed other things to be entered besides IP addresses. This was a common bug that should have not been.

2. Similar to 1. he ran “Showmount –e” found a “trusted” machine that was mounted to Shimomura’s computer.

3. Similar to 1 he ran “rpcinfo –e” and found that it accepted rsh from trusted computers.

4. Found sequence number of 1 + I \text{th} connection = 128,000 +sequence number of \text{I th} connection. This number was useful for sending correct SYN-ACK-ACK to Shimomura’s computer later on.

5. SYN-FLOOD on trusted computer to suppress RESETS; Mitnick sent many SYN messages to not allowing SYN-ACKs to be sent back.

6. Sends spoofed SYN & SYN-ACK-ACK using deciphered seq. number

7. rsh x-term “echo ++>> /.rhosts”; allows anyone to log on to Shimomura’s computer.

8. Takes Oki source code & cleans up log files.
How Mitnick got caught:
- Shimomura was having log files emailed to him; He detected change in length of log files and found out someone has hacked in.
- Bulletin Board “The Well”; reported someone stole the Oki source and was stored in their computers in NC. FBI was also investigating another report concerning a lot of phone calls were made that weren’t being properly charged to NC. So they used directional antennae, scanners and range finders and ran a trace to the calls and found it was coming from an apartment where they presumed Mitnick was living in. They busted into the apartment and captured Mitnick.

Can This Happen Today?
- We don’t use rsh; we use ssh
- No more predictable sequence numbers