**Computer Hacking Techniques and Terms**

1. Brute Force Attack
   1. Terminator, scripts to run through fast
   2. PINs - only 10000 possibilities
   3. Knowledge of password requirements,
   4. Countered with more strict password requirements
2. Password guessing
   1. Most common passwords password, username, 12345, qwerty, letmein, welcome, monkey, abc123
   2. Hints can help lead you toward guessing the password, especially if you know the individual
   3. Username is the password as well
   4. Default password never changed (Cisco routers - admin)
   5. Patterns
      1. If a number is required, add a "1" at the end of common passwords
      2. If a capital is required, capitalize the first letter only of a common password
      3. If a symbol is required, add "!" at the end.
      4. Men use hobbies or interests for passwords
      5. Women use names of people they know.
3. Phishing
   1. Attempting to acquire sensitive info (usernames and passwords) by masquerading as a trustworthy entity in an electronic communication.
   2. Examples
      1. An official looking email from a bank asking for account information verification.
      2. Hyperlinks to websites that contain malware and/or viruses
      3. Especially effective with the elderly and technically challenged.
      4. Social media uses this all the time. Friending someone may give them access to your info.
      5. Target - 110 million customer credit cards stolen through 1 phished subcontractor account. CEO and IT security staff all fired.
      6. Home Depot - 100 million+ credit card numbers phished out.
      7. Nearly 50% of phishing thefts originate out of Russia.
   3. Spear phishing - targeting an individual; gather information first
   4. Clone phishing - Using a previous legitimate email and clone it to mislead the target.
4. Fake Website
   1. Emails or hyperlinks to a website like amazzon.com homedeppot.com
   2. User registers or attempts to login and their username (often email address) and password are obtained.
   3. Most people reuse the same password, so they now can check banks, and other online sites to find where you have accounts that they can infiltrate.
5. Keylogger
   1. Software or hardware that captures keystrokes
   2. Can be used where you have physical access to someone's computer.
   3. Used to get passwords and usernames.
   4. Logs time of day so you can look for first entries each day (when they log in)
6. Garbage Collecting
   1. Dumpster diving for discarded but sensitive information
   2. Some individuals will go through shredded documents
7. Trojan Horse
   1. Refers back to the hollow wooden horse the Greeks hid inside to infiltrate the city of Troy
   2. A computer program that serves a legitimate purpose, but also installs "back doors" on the system.
   3. Some of these may, unknown to the victim, search for credit card numbers, account information, etc… and send the information to the creator of the trojan.
8. Back Door Attack
   1. Not changing a default password would be an example of a backdoor
   2. Some viruses will create backdoor if they are able to work their way onto a network or computer.
   3. Some of these attacks are used to send spam e-mails from the infected computer.
9. DoS attack
   1. Denial Of Service Attack
   2. Essentially the targeted computer is bombarded with endless junk information.
   3. The idea is to consume all bandwidth with the garbage data, so they are unable to transmit anything.
   4. Often the excuse for First person shooters when they get pwned.
10. Smurfing
    1. A type of DOS attack that targets an entire network.
    2. The source IP address is faked and broadcast to all devices on a network continuously, which prevents anyone on that network from transmitting information.
    3. ARP attack at EK. My heroic actions to bring down the infiltrator.
11. Packet sniffing
    1. Using a program like WireShark, a user can see all traffic on the network, even that information that isn't directed at their computer.
    2. They can decrypt the data and extract information they aren't supposed to have.
12. Fake Wireless Access Points
    1. Also called a honeypot.
    2. People set up a fake access point at crowded areas (airports, restaurants, stadiums) where people what free wifi.
    3. Anyone that connects to the wireless network is vulnerable for system scans.
    4. This work on cell phones also!
13. Cookie theft
    1. When you visit a website, your session information is often stored in a cookie. This lets you quickly resume your work or transaction there if you return.
    2. By stealing your cookies, another user can use them to impersonate you, gaining access to account information, even credit card information.
14. Doxing
    1. When sensitive information about an individual is posted in a public forum for all to see.

**Other terms**

White hat - Ethical hacker, often hired to find weaknesses in a company's network security.

Black hat - Hacking for evil purposes and personal gain, usually at another's expense.