**Computer Hacking Techniques and Terms**

1. Brute Force Attack
	1. Automated attack that runs through all possible password combinations.
	2. Bank ATMs - 4 Digit code has only 10,000 combinations
	3. Knowledge of password/username requirements is needed.
	4. Countered by more strict password requirements and lock-outs after failed attempts.
2. Password guessing
	1. Most common passwords: password, username, 12345, qwerty, letmein, abc123, monkey
	2. Hints can help lead a hacker to guessing your password, especially if they know you.
	3. Default passwords are often left unchanged. (Linksys router - admin)
	4. Men use hobbies or interests for passwords.
	5. Women use names of relative or loved ones.
3. Phishing
	1. Attempting to acquire sensitive information by masquerading as a trustworthy entity.
	2. Large numbers of contacts are used to find a victim.
	3. Especially effective against the elderly and technologically challenged.
	4. Examples
		1. An officially looking email from a bank asking for account verification.
		2. Hyperlinks to websites that contain malware/viruses.
		3. Social media uses phishing all the time. Friending an unknown is bad.
		4. Target - 110 million customer credit cards stolen due to 1 phished account.
		5. Nearly 50% of all phishing attempts originate out of Russia.
	5. Spear phishing - Target an individual; gather information ahead of time.
	6. Clone phishing - Using a legitimate email and clone it to mislead the target.
4. Fake Website
	1. Emails or hyperlinks to a website like amazzon.com or homedeppot.com
	2. Fake website looks like the original with login/password fields.
	3. You enter your info and they have the ability now to log into your amazon.com account.
	4. Most people reuse passwords, so they will try the same combination of email/password on other popular sites.
5. Keylogger
	1. Software or hardware the captures keystrokes.
	2. Often times looks like a mini flash drive
	3. Requires physical access to the computer.
	4. Logs time of day, so you can look for first entries of day for login info.
6. Garbage Collecting
	1. Dumpster diving for discarded but sensitive information
	2. Some individuals will go through shredded documents.
7. Trojan Horse
	1. Refers to a 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 "malware".
	3. These "hidden" programs may search for credit card information or account info to send back to the creator of the trojan horse.
8. Back Door Attack
	1. An alternative way to access a computer or network.
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 garbage data, so nothing else can transmit.
	4. Often the excuse of FPS players who get "pwned".
10. Smurfing
	1. A hacking attempt that "spoofs" the source IP address to avoid getting in trouble.
11. Packet sniffing
	1. Using a program like WireShark, a user can see all network traffic, even if it isn't directed to them.
	2. They can decrypt the data and extract info they aren't supposed to have.
12. Fake Wireless Access Points
	1. Also called a "honeypot".
	2. People set up a fake "wifi" hot spot in a crowded area. (airport, stadium, restaurant)
	3. They name the spot after the location. (Gerald R Ford Free Wifi)
	4. Anyone that connects is vulnerable to system scans.
	5. Also works on cell phones.
13. Cookie theft
	1. When you visit a website, your session info is stored in a "cookie".
	2. Cookies allow you to resume work, autofill fields, etc… on a website.
	3. By stealing their cookies, another user can use them to impersonate you, gaining account access, etc..
14. Doxing
	1. When sensitive information about an individual is posted publicly for all to see.

**Other terms**

White hat - Ethical hacker. Often hired by companies to find weaknesses in their network security.

Black hat - Hacking for personal gain, usually at the expense of another person.