Lesson 1

Passwords

Hashing

* Turns plaintext into unreadable jumble
* A password is provided and turned into a hashed value
* Without access to the hash function, you cannot find the password
* Rainbow tables could theoretically store every possible hashed value, however this would take literal Petabytes of storage
* Should lack a pattern
* When credentials are stored as hashes, they are harder to access
* When a user signs in, their password is hashed and compared to the hashed password, to avoid storing plaintext passwords
* Salting is the process of sprinkling a value into a hash function to change it a little
* Passwords should be hashed and salted
* One-way hash functions take a string and output a fixed length hash
* This way the hash holder will never know the original password

Codes

* Cryptography is the study of securely transmitting data
* Codes convert words into less readable formats
* Encoding takes text and transforms it to codetext
* Decoding transforms codetext into text

Ciphers

* Take plaintext and turn it into ciphertext
* Encryption is turning plaintext into ciphertext
* Decryption is turning ciphertext into plaintext

Keys

* Keys are really big strings used in ciphering
* Secret-key cryptography involves passing a key and the plaintext to the user and receiver
* Both sides have access to the key

Public Key Cryptography

* Sender uses a public key and plaintext to create ciphertext
* Then the sender uses a secret key to decipher text
* RSA is the standard

Key Exchange

* Diffe-Hellman
* G and p are agreed on
* A and B have a secret value each
* They have their own private keys

Signature

* Document content is hashed
* Private key and the hash are hashed
* Decrypted hash value should match initial value

Passkeys

* Generates a public and private key
* Public key to website
* Then passes the private key and challenge value
* Algorithm returns signature

Encryption In Transit

* Securing data as it communicates back and forth
* End-to-End encryption ensures no third parties read the transiting data

Deletion

* Secure deletion changes the values of deleted files to ones or zeros
* Most OS's just forget where the file is

Full Disk Encryption

* Encrypts the entire HDD or SSD
* If it is stolen it cannot be accessed
* You could forget the password
* This can be used to do ransomware

Quantum Computing

* Really fast at guessing passwords

Lesson 2

WIFI

* Secured networks use encryption
* WPA or WIFI Protected Access is a form of encryption on WIFI networks

HTTP

* Unencrypted
* Vulnerable to many attacks

HTTPS

* Traffic between parties is encrypted
* Accomplished by TLS and public key cryptography
* Websites have an X.509 certificate which gives a private key
* Certificate Authorities (CA) issue certificates
* Browser creates a hash
* Then uses a public key to verify the hash
* If these are verified, then it is secure
* HTTPS is generally good, however there are exceptions
* SSL Stripping can redirect to HTTP
* HSTS makes the browser only direct to HTTPS

VPN

* All traffic is encrypted
* Used to pretend to be in another country

SSH

* SSH commands can be issued to remote servers
* Still need credentials to connect

Ports

* Port numbers direct to a specific server
* Port scanning attacks look for all open ports
* Firewalls prevent port attacks
* Uses IP to prevent outsiders from using secured ports
* Deep packet inspection examines the content in packets
* Deep packet goes via proxy which assumes control for you

Malware

* Software which compromises computer security
* Viruses infect the computer and can do stuff
* Worms infect a computer and spread
* A botnet can infect, spread and execute commands
* Botnets can do DDOS against servers which shut them down

Antivirus

* Detects viruses and removes them (hopefully)
* Automatic updates
* Vulnerable to zero-day attacks which exploit unknown vulnerabilities