CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-2-types_of_attacks
Title: Types of Attacks
Subtitle: CompTIA Security+ (SY0-501)

1.2 Types of Attacks

- 1.2 Compare and contrast types of attacks.
  - Social engineering
    - Phishing
      - Basic scam aimed at as many people they can
      - Using for example, brand trust like Walmart, Google, PayPal....etc
    - Spear phishing
      - More sophisticated phishing attack
      - Appears to come from a relative, friend, co-worker, your bank,
      - Involves some reconnaissance
    - Whaling
      - Most sophisticated phishing attack
      - Attacker(s) assume the identity of a C'level employee such as CEO or CFO, company attorney using insider threat actors
    - Vishing
      - A phishing attack carried out via voice technologies
      - Landline, VoIP, Voice mail/message, cell phone
      - Example
        - Victim is warned out potential suspicious activities on credit card accounts, bank accounts, mortgage accounts...etc
    - Tailgating
    - Impersonation
    - Dumpster diving
    - Shoulder surfing
    - Hoax
    - Watering hole attack
      - This attack targets a group of people that work together by infecting websites that the group is known to visit. It only takes a single user to get infected to gain access to the network.
    - Principles (reasons for effectiveness)
      - Authority
        - People are conditioned to respond to authority
      - Intimidation
        - Using implied authority for means of propagating an attack
        - Two higher ranking military personel
      - Consensus
        - When a user does not know how to react (say to an email), so they will look to others to see how to react (to click the email, to respond to the email)
      - Scarcity
        - People are more likely to respond to scams when there is a time or availability concern
        - Download "this add-on" to view the page
        - Not being able to view a page until a program to install can make the victim see it even more.
      - Familiarity
        - People are comfortable with those they are familiar with
      - Trust
        - First objective is to establish trust
      - Urgency
    - Application/service attacks
      - DoS
      - DDoS(diagram)
      - Man-in-the-middle
      - Buffer overflow
      - Injection
      - Cross-site scripting
        - Malicious script embedded in a trusted web application that is executed against a victim
        - Redirect the user, extract private data
      - Cross-site request forgery
        - The users browswer is forced to attack the website performing, for example fund transfers, email address changes
        - So the user sends malicious requests to the website(by the malicious script)
      - Privilege escalation
      - ARP poisoning(diagram)
      - Amplification(Increasing the payload)
      - DNS poisoning(diagram)
      - Domain hijacking
        - Transference of a domain from the original owner, purchaser to another registrar through malicious or fradualent means
        - Often go undisputed

        - Hard to reverse
        - ICANN’s Registrar Transfer Dispute Resolution Policy to seek the return of the domain
        - http://huff.to/2odPlpx
        - http://mla.com/
    - Man-in-the-browser
    - Zero day
    - Replay(diagram)
    - Pass the hash
        - Authenticate with a hash value rather than the actual typed password
    - Hijacking and related attacks(diagram)
        - Clickjacking
            - Placing hidden links on seemingly legit images or clickable content that redirect the victim to an unintended location
        - Session hijacking
        - URL hijacking(same as typo squatting)
        - Typo squatting(same as url hijacking)
            - relies on Internet users to mispell the URL or web address in the browser
    - Driver manipulation
        - Shimming
            - Works the same way as application shimming
            - However drivers typically operate in kernal mode so like rootkits they can be devastating
            - Credit card shimming works the same way by intercepts communications between the card and the reader (EMV Standard-Europay, Mastercard and Visa)
            - Implement driver-signature enforcement
        - Refactoring
    - MAC spoofing(diagram)(ARP Poisoning)
    - IP spoofing(mention in context of spoofing)
- Wireless attacks
    - Replay
    - IV
    - Evil twin
    - Rogue AP
    - Jamming
    - WPS
    - Bluejacking
    - Bluesnarfing
    - RFID
    - NFC
        - Based off of different standards including:
            - RFID, proximity cards, identification card, contactless ICs, smart cards
            - Standardization of international interoperability
            - Examples
                - eavesdropping
                - data modification
                - replay attacks
                - data corruption/manipulation
                - MiTM
                - Spoofing
                - Mobile malware
    - Disassociation(form of DoS)
        - Also deauthentication attack
        - airdump-ng, aircrack-ng
- Cryptographic attacks
    - Birthday
        - Based off of the birthday paradox
        - Out of a random gathering group of 23 people there is a 50% chance that two people will have the same birthday.
        - A type of hash collision attack that seeks to make it easier to brute force
        - With a GIVEN hash it is much harder to find a collision
        - It is easier to find a collision for ANY to hash values
    - Known plain text/cipher text
        - Known plaintext attack
        - Known ciphertext attack
            - only two pieces ciphertext are available without or very little knowledge of the plaintext input(attacker might know the language of the plaintext)
            - Examples
                - PPTP used RC4 stream with the same key on each end
                - WEP was very susceptible to known ciphertext attacks
    - Rainbow tables
        - precomputated table to assist in cracking of password hashes
    - Dictionary
        - seeks to defeat password-based authentication mechanisms
        - a method of attack that systematically enters all the words in a dictionary
    - Brute force

  - Online vs. offline
- Collision
  - NTLM
  - MD5
  - SHA1(theoretical)
    - http://bit.ly/2oqG4e3
- Downgrade
  - Try to get a system to negotiate the use of a protocol of weaker security strength
  - Think of backward compatibility, only the purpose is to crack the weaker security protocol or suite.
- Replay
- Weak implementations
  - Shorter key lengths
  - Passwords vs certificate
  - Single Factor (SFA) vs Multi Factor(MFA)
  - WPS vs WPA2
  - WEP vs WPA2
  - WPA2 Personal vs WPA2 Enterprise
  - MD5 vs SHA1
  - SHA1 vs SHA256