# CompTia Notes: Threats and Vulnerabilities

* Types of Malware
  + Virus
    - Requires User interaction to install and replicate
  + Spyware
    - Captures user activity
  + Trojan & Remote Access Tools
    - Disguised as something safe
    - RATS allow full access and control to system
  + Rootkits
    - Load before the system loads
    - Allows them to bypass antivirus
    - Can use TDSSkiller to remove
  + Back doors
    - Software that installs for the purpose of installing other software
  + Logic Bomb
    - Triggers after a time or specific activity
    - Can accidentally be backed up while dormant
  + Botnets
    - Infect large numbers of computers to launch a large scale attack (DDoS)
  + Ransomware
    - Scares a person into doing something
    - Usually locks up files
  + Polymorphic and Armored Malware
    - Changes each time it is installed to avoid detection
    - Avoids by encryption, obfuscation, and additional useless code
* Types of attacks
  + Man in the middle
    - A person uses Wireshark to capture info being passed on a network
    - Can get a hash of a PW and then brute force the PW hash
  + DDoS
    - Uses Botnets, Bot herders, and a Command and Control Center
  + Smurf Attack
    - Similar to DDoS
    - Victims IP address is spoofed (attacker assumes IP address of a victim) and ICMP (internet control method protocol or PING) messages are broadcast to a computer network
    - Recipients will respond with reply to victims IP address, flooding it with responses
    - Will slow the target PC to point of being unusable
    - Mitigation: can set policy to disallow computers from responding to ICMP requests or broadcasts
    - Configure routers to not forward broadcasts (default on most routers)
  + Spoofing
    - Pretending to be another IP address
    - Can be used with MiTM attacks to intercept traffic and impersonate one person
  + Spam
    - Spam attacks can be launched like traditional DDoS attacks
    - Thousands of millions of botnet computers can be controlled to send spam email messages to an email server
    - Can degrade email server performance or take server offline
  + Phishing
  + Target email or websites that contain malicious links masqueraded to look like legitimate links
  + Designed to steal credentials, money, personal information
  + Tell-tale signs of phishing:
    - Bad grammar
    - Threats
    - Masked email links
  + SPiM
    - Spam over instant messaging
    - Usually contains unsolicited advertising and/or links to websites
  + Vishing
    - Voice Phishing
    - Social engineering techniques designed to get victim to divulge information
    - Attacker poses as legitimate company, repair person, security personnel or someone of trust
  + Spear Phishing
    - More targeted and focused phishing campaign
    - Appears to come from someone within the targets company in a position of authority
    - Target campaign that relies on familiarity to trick the victim into clicking on a link
  + Xmas attack
    - A scan of a host to determine if its online and what responses are provided can help determine what type of system it is
    - Set a number of TCP Flags that light up like a Christmas tree
    - Nmap lights up certain flags
  + Pharming
    - Redirect a websites traffic to somewhere else
    - Can be accomplished by modifying the host file or the router
    - Also known as DNS poisoning or ARP Poisoning
  + Privilege Escalation
    - Obtain elevated privileges on the target
      * Dump the SAM (local account file)
      * Retrieve password file
      * Look of insecure file shares
      * DLL pre-loading
      * Insecure or weak security on processes
    - Many vulnerabilities enable an attacker to gain system-level permissions
  + Malicious Insider Threat
    - Threats from internal employees who may have access to sensitive data or the ability to cripple network functionality, key systems, etc.
    - Plant logic bombs, time bombs, etc.
    - Siphon confidential information
      * Espionage
      * Financial gain
      * Loss of trust or public opinion
  + Transitive access
    - If A trusts B and B trusts C, then A trusts C
    - Can make it difficult to track permissions
  + Client-side attack
    - Attack where the connection to malicious content is initiated from the client
    - Usually from being enticed to click on a malicious link in email
  + Password attacks
    - Brute Force:
      * try every possible combination of alphanumeric characters, upper and lower case
      * Very slow
      * Most accounts will lock out after “x” number of attempts
    - Dictionary:
      * Feeding a brute-force password cracking too l a list of known words, phrases, etc.
      * Tries subset with higher likelihood of success
      * Tools:
        + Brutus, Cain and Able, Crack, Ophcrack
    - Hybrid
      * Tries list of words, then combination, then variation, combination of brute force and dictionary
    - Birthday
      * Wroks on cryptographic phenomenon of hash collisions
      * Given enough time, two independent sources could yield the same hash, rate of occurrence varies depending on hash algorithm
      * From Birthday paradox
      * Just find another word with a matching hash and use that as the PW instead
    - Rainbow
      * Precomputed table to reverse cryptographic hashes
        + Reduce time to brute-force a pw
        + Different table needed for each hash type (MD5, SHA1)
      * Can be mitigated using Password salting
        + Adding random data to the hashing algorithm so that each users hash is unique even if both have the same password
        + Larger salts increase security
    - Typo Squatting
      * Someone sets up domain name with slight typo for a popular website
    - Watering hole attack
      * Sophisticated attack that identifies less secure websites users in a particular company or organization are likely to visit
      * Attackers plant malware on the sites users visit to infect the targeted users once they visit the infected site
      * Malicious code scans the users’ computer for vulnerabilities
      * May download additional code to initiate attacks, siphon data, etc.
* Effectiveness of Social Engineering attacks
  + What is social engineering?
    - Asking seemingly non-invasive or unimportant questions to gather information over time
    - Gain Trust
    - Reduce defenses
    - Can be combined with other techniques to gather sensitive information
    - Use information to get more information
  + Shoulder Surfing
    - Strike up a conversation about their kid’s sports, then ask to see some pictures
    - Should surf as they enter their username/password into social media website
    - Mitigation
      * Privacy screens
      * Masked passwords (put multiple asterisk per key stroke further obfuscate the length of a password)
      * Cameras to monitor doors, key card access, etc.
  + Dumpster Diving
    - Removing trash from dumpsters that could reveal sensitive information
      * Usernames/ passwords
      * Personally identifiable information
      * Resumes
    - Mitigation:
      * Shred documents
      * Locked waste cans to be transported off-site for shredding/disposal
  + Tailgating
    - Someone who comes in behind and authorized user and gains entry by entering right behind them
    - Social engineering techniques that relies on a person’s good nature
    - Bad actor seems to know what they’re doing, is fumbling around for badge, speaks the proper lingo, etc.
    - Mitigation:
      * Man traps, guards, CCTV, Security awareness is also key to instill inherence to proper procedures.
  + Impersonation
    - Hacker fools the target by acting like an authorized person, repair technician, remote employee
    - Social engineer may spend time learning about the company, lingo, people in other offices, key names to drop, etc.
  + Hoaxes
  + Whaling
    - Targeted phishing and spear phishing techniques aimed at “big fish” like company executives
    - Emails are targeted, very specific, and seem legitimate
  + Vishing
    - Voice Phishing
  + Principles
  + Authority
    - Hacker appears to know what they’re talking about or has special knowledge of the company.
    - Technical jargon
    - Name dropping
    - Knowledge of specific systems/ applications
  + Intimidation
    - Hackers impose their will on the target by:
      * Threatening negative action
      * Threaten to release sensitive information
      * Cane be combined with scarcity and urgency
  + Consensus/social proof
    - Mob Mentality
    - Trick people to believe they are in alignment with the larger group
  + Familiarity/ Liking
    - People are more likely to interact with people they’re already familiar with
    - Puts people at ease to gain more information
    - Attacker will establish a common contact or friend to establish trust
  + Trust
  + Scarcity/Urgency
    - Elicit action to get victim to act quickly
    - Time based offer
    - Issue that needs to be resolved quickly.
* Wireless Attacks
  + Rogue Access Points and Captive Portals
    - Unauthorized access point
    - Installed in a network by unauthorized personnel
    - Can be used in a Man in the Middle Attack
    - Evil Twin: Rogue access point that impersonates another access point by using the same ESSID, potentially jamming the legitimate access point
  + War Driving and War Chalking
  + Bluejacking and Bluesnarfing
    - Bluejacking: Sending of unauthorized messages or data via Bluetooth technology
    - Typically sending a vCard with contains a message in the name field to another Bluetooth enabled device via the OBEX (Object Exchange) protocol
    - Has to be discoverable
    - Bluesnarfing: pulling data off the victim’s device
    - Contact lists, pictures, messages, emails, Personally identifiable information
  + IV attacks
    - Initialization vector attack
    - Weaker encryption had short IVs that would repeat fairly quickly
    - Attacker could flood the network, sniff the packets and see the IVs being sent
    - WEP uses a 24-bit IV, easily cracked, why WEP shouldn’t be used
  + Packet Sniffing
    - Wireshark
    - Gain information about traffic traveling the network
  + Near Field Communication
    - Technology to allow communication between devices within close proximity to each other
  + Replay Attacks
    - During sniffing, a replay attack captures packets and puts them back on the wire
    - Packets can potentially be modified and retransmitted to look like legitimate packets
    - Sequencing helps mitigate the effectiveness of this type of attack
  + WPS Attacks
    - Easy to setup “pushbutton” WPA security between devices
    - First introduced in 2006 but serious bug was discovered in 2011
    - Pin can easily be cracked in 3-5 hours typically using various techniques
    - REAVER and BULLY are linux pen-testing tools
    - Installed with Kali Linux by default
    - To mitigate, update routers
  + WEP and WPA Attacks
    - Since WEP and WPA are both weak encryption, use a strong pre-shared key or RADIUS authentication
* Application Attacks
  + Cross-site Scripting
    - Non-persistent: Specially crafted URLS sent in an e-mail, instant message, blog post
    - DOM based: Can be non-persistent or persistent and used to hijack sessions
    - Persistent: server based and can execute on a user’s computer just by visiting an infected website
    - User gets an email with a link, the link goes to a website that has malicious code imbedded in it
    - The browser runs malicious code because it was served from a site it trusts
  + Cross-Site Request Forgery
    - Attacker gives user a link, the user clicks on it, the user goes to the attacker’s server, the server pulls the cookie off the user’s session and goes to their bank with it to get access to their banks data where they then transfer money out
    - The server performs an action because it was send a request from a client it trusts
  + SQL and CML injection Attacks
    - Modify SQL query to bypass login screens, have the website return table info like usernames, passwords, etc. Cause the application to throw an error and crash, allowing an attacker remote access or return info
    - LDAP: Lightweight Directory Access Protocol
      * Address Book of user accounts used to authenticate users
      * Identifies level of access, group memberships
      * Similar to SQL injection attacks in the query
    - XLM Injection: Attack technique that manipulates the logic of an CLM application or service
    - Fuzzing
      * Used by application designers to find bugs, defects, and security holes in application
      * Hackers use fuzzing techniques to identify zero day vulnerabilities and crash applications/websites
    - Must sanitize/validate inputs in the backend to mitigate
    - Exploit-me and metasploit can be used to help sanitize inputs
  + Directory Traversal/ Command Injection
    - Attack that manipulates user input to cause the application to traverse a directory structure and access files not intended to be visible
    - Dot slash attack, directory climbing, backtracking
  + Buffer Overflow Attacks
    - Causes a system or app to crash or behave unexpectedly
    - Writing more data than the buffer can handle
    - Data is written to adjacent memory
    - Calls or pointers to jump to a different address than what was intended
    - Can contain user executable code which could allow remote code execution
  + Integer Overflow attacks
    - Crash a program using larger values than the application expects and can handle
  + Zero-day attacks
    - Vulnerabilities that are discovered and exploited before the developer has a chance to issue a patch or fix
    - Some groups horde zero-day exploits to use later
  + Cookies and Attachments
    - Cookies contain information about the user including website history, browser settings, etc. to customize the user experience
    - Data can be accessed and used by 3rd parties
  + Locally Shared Objects (LSO)
    - Like Flash cookie, not typically deleted when you clear cookies from your system
    - Can be used to track a user’s browsing habits and is shared by all users
  + Flash Cookies
    - Storied by adobe flash, hard to remove
  + Malicious Add-ons
    - Applets that are constructed to steal information or otherwise harm a user or system.
    - Many users don’t understand security implications when an applet prompts to allow access and simply hit accept
  + Session Hijacking
    - Items used to validate a user’s session are compromised and reused by a malicious person
    - Man in the middle attacks
    - Side jacking: initial login may be encrypted but the rest of the session is not and can be captured using packet sniffer by the attacker
    - Fire sheep, backtrack, and Kali-Linux can do this easily
    - Make sure you log out of sessions, encrypt communication when using public Wi-Fi
  + Header Manipulation
    - Hijacking a user’s session using XSRF its possible to change header values, change cookie parameters, etc.
    - Use a VPN to mitigate.
  + Arbitrary/Remote Code Execution
    - Manipulate instruction pointer of a running process to point to the injected code Can run as root/admin or crash the system.
    - Used in tandem with buffer overflow attacks
* Mitigation and Deterrent Techniques
  + Monitoring System Logs
    - Event Logs
    - Audit Logs
    - Security Logs
    - Access Logs
    - Useful in Analysis, Forensic Investigations, Trending, Alerting, Monitoring of Activity
  + Hardening Systems and Applications
    - Getting rid of things that aren’t necessary, limits attack vectors
    - Protect management interfaces and applications
    - Password protection, fine line between secure and overly complex that users write them down
    - Disabling unnecessary accounts
    - Don’t give regular users access to administrative tools
  + Network Security
    - MAC address = media access control address
    - 48-bit hex number that is hard coded on a NIC
    - 802.1x Extensible authentication access protocol over LAN
    - Three Components: Supplicant (host) Authenticator (switch) Authentication Server (RADIUS)
    - Disabling Unused Interfaces and Services
  + Rogue Machine Detection
    - Identify people who don’t belong on the network
  + Security Posture
    - Continues security monitoring
    - Keep constantly updated and monitor systems
    - Remediation, dependent on severity
  + Reporting
    - Alarms, Alerts, and trends
  + Detection vs Prevention Controls
    - IDS - Intrusion Detection System, common, easy to set up, log alerts and events for later analysis, reactive
    - IPS – intrusion Prevention System, newer, enables prevention such as blocking IP address, false positives could block legitimate access.
    - Cameras and guards
* Discovering Security Threats and Vulnerabilities
  + Setting a baseline is important to compare against
  + Protocol Analyzers and Vulnerability Scanners
    - Packet Sniffers, captures packets as they traverse a network
    - Will show vulnerability scanners and give advice on how to quarantine and fix
    - Passively Test Security Controls
    - Interpret Results
    - Identity vulnerabilities
    - Identify lack of security controls
    - Identify common misconfigurations
  + Honeypots and Honey nets
    - Leave vulnerabilities open to attract hackers
    - Make it appear to have sensitive information
    - Monitored to identify hackers and their methods and techniques
    - Honey net is larger scale, network set up intentionally for attack
    - Then used to harden the rest of our environment
  + Port Scanners
    - Scans a range of IP addresses for open ports
    - Fingerprints what type of OS, application and services a host is running
    - Best to run scan and shut down ports that aren’t used
  + Banner Grabbing
    - Used to provide information about a service running on a particular port
    - Probe common service ports to search for vulnerable services and versions
    - Tools: Telnet and netcat
  + Passive vs. Active Tools
    - Passive: Don’t interact directly with the hosts, gather information and report externally, packet captures/sniffers, not usually visible
    - Active: Penetration testing Port Scanners, Honeypots, Banner Grabbing
  + Risk Calculations
    - Threat vs. Likelihood: is the juice worth the squeeze
    - Business will determine risk tolerance
    - Annual loss expectance (ALE): Monetary measure of how much loss you can expect in a year
    - Single Loss Expectancy (SLE): How much you expect to lose at any one time
      * Asset Value x Exposure Factor
    - Annualized rate of occurrence(ARO): Likelihood of an event occurring within a year
    - SLE x ARO = ALE
  + Assessment Types
    - Risk:
      * What is the danger
      * How likely is it
    - Threat
      * Likely dangers associated with risk
      * Means and source of potential attack
    - Vulnerability
      * Where are the gaps and how quickly can you fix them?
  + Assessment Techniques and Baseline Reporting
    - Baseline: determine how things should be operated
    - Detect changes from baseline
  + Code Review
    - Review custom written code to determine gaps and security holes
    - Protect against SQL, XML, LDAP injection vulnerabilities
    - XSS and XSRF vulnerabilities
    - Scanning code can be automated with software
  + Determine Attack Surface
    - Determine what area of an application is available to users
    - If a vulnerability exists, but users can’t reach it, then it is lower priority
    - What services, ports, protocols, interfaces, etc. are being used
    - Disable and turn off unnecessary functions, ports, etc.
  + Review Architecture
    - Review entire stack top to bottom, web, middleware, database, etc.
  + Review Designs
    - Useful when merging companies using different systems
    - Makes sure there aren’t gaps and vulnerabilities in something that gets used by something secure
* Penetration Testing vs. Vulnerability Scanning
  + Verifying threats and bypassing security controls
    - Verify the security controls are in place and functioning, then try bypass
    - Nmap, Netcat, Metasploit, Kali-Linux
    - XSS attacks, IP or MAC Spoofing
  + Actively Testing Security Controls
    - Penetration testing performs intrusive tests, could disrupt business operations like a real attack
    - Exploits vulnerabilities found during the vulnerability scan
    - Vulnerability scanning identifies gaps and holes in defenses
  + Exploiting Vulnerabilities
    - Nessus and metasploit will identify vulnerabilities, missing patches, misconfigurations, etc.
  + Vulnerability Scanning
    - Should be performed in tandem with pentesting
    - Non-intrusive and can be performed with credentials or without credentials depending on the risk tolerance
  + Testing Security Controls and Identifying Vulnerabilities
    - A good vulnerability assessment will show vulnerabilities
    - Might just be something that is not a best practice, missing patch, or completely missing
    - Interview personnel
    - Review logs
  + Identify Common Misconfigurations
    - Review logs and perform audits of key assets
    - Nessus and Metasploit will identify security misconfigurations
    - Also identify when things were changed
  + Intrusive. Non-intrusive and Credentialed vs. non-credentialed
    - Intrusive testing can disrupt normal operations or have a greater impact of reducing system responsiveness
    - Attackers typically start out with non-credentialed access
    - They normally don’t know much about the networks they’re attacking
    - Attackers try to gain privileged account access
  + False Positive
    - Try limit to make sure resources are utilized efficiently
  + Black, white, and gray box testing
    - Black box: tester has no prior knowledge of the network or environment, no documentation, no account information, will use fuzzing techniques and injection attacks
    - White box: full knowledge of environment, possibly a disgruntled employee, might have source code and log in info
    - Gray Box: Some knowledge of environment, no access to documentation or data,
  + Things to remember
    - Obtain consent in writing if possible, might be considered an attack and grounds for dismissal
    - Review company guidelines and rules of engagement
    - Identify and assess tester’s skills and background
      * Verify and obtain references when possible
      * Tester could potentially have access to sensitive corporate data