Cyber Security and Cyber Forensics (Chapter - 4 : DISSA Course) **Part 1; Introduction**

Arijit Chakraborty

Feb 20, 2022

Hacking types

- **Social Engineering** - **entrapping someone with intent** to gain personal & sensitive information - User name passwords & Credit card details.
- **SQL Injection** - code injection technique for attacking data-driven applications on which malicious SQL statements are affixed to entry field to execute.
- **SQL Injections : Aim :** For **dumping complete database** of system
- For performing **various queries that are not permitted** by application
- For **changing content** of a database
- Injections = placed on search fields, address bars, and data fields.
- Make use of the " ' " characters in string

✓ **Retrieving hidden data**, modify SQL query to return additional results.

✓ **Subverting application logic**, - can change query to interfere with app's logic.

✓ **Examining database**, - extract information about version structure of database.

- **Spyware** - software with **purpose to obtain information** regarding organization or person without their assent
- **Trojan** - malicious programs **masked to be like valid programs** to make it harder for differentiating them - alter information, destroy files, or steal passwords or information

Hacking terms

- **Adware** - Software used for pushing pre-chosen ads to be displayed on system.
- **Back Door** - aka ‘trap door’, = hidden entry for malware - affect security measures - logins & password protections.
- **Botnet** - aka ‘Zombie Army’, computers controlled without knowledge of owners.
- Botnets used for sending denial or spam service attacks.
- **Brute Force Attacks** - simplest & automated kind of method for obtaining access from system or website.
- tries various combination of passwords, usernames, again & again until entry obtained
- **Denial of Service attack (DoS)** - malicious pursuit for making network resource or server unavailable for users, by disrupting or suspending services of hosted connection of Internet.
- **Logic Bomb** - Virus stashed into system provokes malicious action where few conditions are met. General version = time bomb.
- **Keystroke Logging** - tracking the keys found in computer.
- used by Black & Gray hat hackers for recording login IDs & Passwords.

Attacks

- **Malware -**
- different forms of **intrusive or hostile software** - worms, computer viruses, Trojan horses, Spyware, Ransomware, Scareware, Adware etc
- **Phishing -**
- **e-mail fraud method** -- perpetrator pushes out legitimate-looking email to obtain financial & personal information from victims
- **Spam -**
- unsolicited email aka junk mail sent to vast number of recipients
- **Spoofing -**
- used for obtaining **unauthorized access to computers** -intruder forwards message to computer with IP address , denotes that text coming from trusted host.

Attack Descriptions

- **Denial-of-service (DoS)** –
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS)** –
- a coordinated stream of requests is launched against a target from many locations at the same time

Attack Descriptions

- **Spoofing -** technique used to gain unauthorized access whereby = intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network

LOG4J vulnerability- 2021

- Log4Shell, an internet vulnerability that affects millions of computers, involves obscure but nearly ubiquitous piece of software, Log4j.
- The software is used to record all manner of activities that go on under the hood in a wide range of computer systems.
- Log4j records events – errors and routine system operations – and communicates diagnostic messages about them to system administrators and users.
- First came to widespread attention on Dec. 10, 2021, Hackers using the vulnerability.

Mobile hacking

- **Key Features**
- Track location and sim card activity
- Check messages & calls
- View media files
- Hidden details - passwords , usernames, browser history,
- ● Control remotely
- 1. **Ultimate Phone Spy**
- Features - , sent & received messages, social media activities, browsing history, etc.
- inbuilt GPS tracker implanted - even track location of targeted device

Cyber incidents

- **Gaming industry**
- 152 million web application attacks & billions of incidents of credential stuffing over a 2-year period.
- Gaming industry suffered 12 billion cyberattacks between Nov 2017 - March 2019

Online gaming – IT Risks

- risks from social interactions with strangers who may trick user into revealing personal or financial information
- risks from computer intruders exploiting security vulnerabilities
- risks from online and real-world predators
- risks from viruses, Trojan horses, computer worms, and spyware

- **Black Hat Hackers**
- Crackers who perform **hacking activity with intent of obtaining unauthorized access** to system & causing a threat to its operation for stealing confidential information.
- Black Hat Hackers = always **considered illegal** because of malicious intent.
- **invade into system or network** for stealing info or money.
- Can send Spam emails by using victim's server to any email address
- Black Hat Hacker = person behind computer **who aims to find vulnerability in networks or computer** & break into it.

Grey Hat Hackers

- Hackers who have blend of **both White and Black hat hackers**.
- usually **surf into internet for looking at vulnerable threats** in System, Networks, Phone system, or Computers.
- Once they identify vulnerability, **then they hack into them & fix it.**
- Later they inform System Administrator what they do & charge a small fee for identifying the threat & fixing it.
- **Spy Hackers**
- recruited mostly in corporations for infiltrating business secrets, trading, & competition.
- Spy Hackers use same tactics like hacktivist **– but : motto of these hackers** = meet goal of client & complete assigned task.

Trojan Horse

- **Software may appear legit might be trojan**.
- A PDF / Avi contain trojan.
- Trojan horses runs in background process,
- collect information & send it to hacker.
- Trojan horses can be sent via- pen drive, ipod, website or email.
-

Password Hacking

- passwords for databases, emails, bank accounts, computer systems, servers.
- **Strong password :**
- Consists of 8 Characters
- Mix of numbers, special characters, letters
- Combination of capital & small letters.

Password hacking techniques

- **Dictionary Attack**
- hacker uses **predefined set of words from dictionary** for **guessing** passwords. When **passwords are weak**, easy for dictionary attack to decode them fast
- **Hybrid Dictionary Attack**
- makes use of **group of dictionary words** combined with **extensions.**
- Ex: word "admin" joins itself with extensions like "admin15" & " admin157",
- **Brute - Force Attack**
- hacker shall make use of **all possible sequences of special characters, numbers, numbers, small & capital letters for breaking passwords**.
- has **highest probability** of success,