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

Arijit Chakraborty

June 19 , 2021

Key points

- Indian Users consumed 15 GB p.m – 2020
- Data use / person = 43 times increase in last 6 years
- Malware, spyware
- Cyber threat – ERM
- Rogue software – Boeing case
- IS Audit scope – multi-domain
- IS Audit Standards – industry-specific, regulation-specific
- Audit Reporting format – different

Cyber Threat Signal 2021

- **AusCERT, CERT-In, KrCERT/CC, Sri Lanka CERT|CC**

Global Common Cyber Threat Outlook

- Targeted ransomware attacks becoming more common & damaging
- Attacks on specific targets -- governments & businesses.
- Surge of ransomware attacks - industrial sectors : service, manufacturing & healthcare.
- New aggressive methods to demand ransom, threatening to publish data & encrypting files.

National Cyber Threat Outlook

- 1. **Transformation of Malspam to Masspearing (Australia, AusCERT)**
- The introduction of ‘masspearing’ combining personalized emails & spam campaigns.
- Emotet malware - rise through spam campaigns.
- Personalized attacks on specific corporate individual targets using leaked data such as emails, contract information, etc.

India

- 2. **Cyber-Attacks due to COVID-19 Pandemic Induced Work Culture (India, CERT-In)**
- Attacks **targeting teleworkers** through malicious websites & emails containing malicious attachments.
- Growing risk of **corporate data leakage** from endpoint devices due to **increased teleworking.**
- Attempts to infiltrate **corporate networks** through remote network environments, such as **vulnerable VPNs**

Korea

- **3. Surge of second attacks using dark web data leaks (Republic of Korea, KrCERT/CC)**
- As dark web markets expand, transactions of **sensitive information grow.**
- Surge in sales of network access authorization information – **VPN due** to recent teleworking trend.
- Attackers **collaborate to lower threshold & expand scale** of attack

4. Sri Lanka

- Increasing sophisticated BEC(Business email compromises) (Sri Lanka, Sri Lanka CERT|CC)
- Attacks **targeting export & import businesses.**
- Use of phishing, to attack **corporate mail.**
- Sophisticated attacks, - spoofed or compromised **payment information** to partner accounts of companies.

CYBER CRIMES

- **Cyber Threats-**
- Intrusion for monetary or other benefit
- Interception for espionage/spying
- Manipulation of information or networks
- Data destruction
- Evasion tools and techniques
- IP theft
- Spyware/ Virus/Malware
- Payment Devices- frauds
- Mobile Money Interception

Hacking

- ‘Method of identifying set of vulnerabilities on target system & exploiting them systematically.
- **Ethical Hacking** = ascertains itself from hacking by adding important elements to a process - 'consent'.

1. The Process eventually **becomes a legal activity.**
2. The Ethical **Hacker seeks permission before hacking into a system** - it should be ensured hacking is **performed legally** & hacker **doesn't have any malicious intent**

Why Hacking ?

- Money extortion
- For Fun
- To Show-off
- Stealing confidential information
- To hamper privacy
- To damage System functioning
- To test security of the system

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 the 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.

Ethical hacking

- **Network Hacking** -
- process of obtaining **information of any Network using tools** (Ping, Tracert, NS Lookup, NetStat & Telnet). Networking hacking - performed with **intent to cause a threat to Network system** & hinder operations of network.
- **Website Hacking** -
- act of **getting unauthorized control over Web Server** & related to software like interfaces & databases.

- **Email Hacking -** obtaining **unauthorized access** to Email account & executed without any consent of owner.
- **Password Hacking -** method of **mending secret passwords** from data transmitted by computer system.
- **Computer Hacking -** act of **stealing Computer ID & Password** using hacking methods & gaining unauthorized access to computer system.

Hacking

- **Uses:**
- For recovering **lost information**
- For **executing penetration testing** to intensify network & computer security.
- **Downsides :**

✓ Immense Security Breach.

✓ Hindrances in System operations.

✓ Malicious threats to system.

✓ Unauthorized access to system or private information.

White Hat Hackers (WHH)

- perform Hacking activities **with good intent**.
- **WHH : Computer Security Experts** - specialists in pen testing
- professionals who constantly defend growing technology to fight criminally-minded hackers.
- **Elite Hackers (EH)**
- Masters of all types of Hacking.
- EH – have good reputation
- EH : treated as Senior-level hackers in hacking community.
- Called ***Masters of Hacking & deception.***

- **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.

Ethical hacking steps

- ✓ Reconnaissance
- ✓ Scanning
- ✓ Gaining Access
- ✓ Maintaining Access
- ✓ Cleaning Tracks
- ✓ Reporting
- ✓ Quick Tips

Website details - Domain Name information

- ***http://www.whois.com/whois*** website
- in-depth details of domain name along with - owner, registrar, expiry, date of registration, owner's contact information & name server.

History of a Website

- History of Website using www.archive.org.

Ethical Hacking - Sniffing

- method of capturing packets that pass via specific network using sniffing tools.
- Aka "tapping phone wires" to know details of conversation.
- **What can be sniffed :**
- Email traffic , FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions

Network vulnerabilities

- Ethical Hacker & Pen-tester list vulnerabilities identified on network.
- Port Scanning
- Vulnerability Scanning
- **Network Scanning -**

The hacker seeks the open ports.

✓ Scanning the vulnerability

✓ Scanning beyond the IDS

✓ Preparing proxies

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 in any form - pen drive, ipod, website or email.
- **Trojan records Gmail password that victim types & send it to Gmail hacker**

Use of Trojan

- Trojan can utilize **victim's computer** for attacking other system
- Trojan **steal financial data** - transaction details & bank account details.
- Trojan **encrypts all files & hacker henceforth demand money** that is required for decrypting it. = Ransomware Trojans.
- Can use phones for sending SMS to third parties. = SMS Trojans.

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 number of extensions like "admin15" & " admin157", etc.
- **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,
- needs more time for processing all types of sequences.

Browser Password Manager

- Popular browsers such as Chrome and Firefox often used to store passwords.
- **Easy to hack passwords** stored in browser.
- **Select** ‘Saved Passwords’ option & find passwords of all email accounts.

- **Bogus software updates**
- Hackers may send fake updates that actually install malicious backdoor programs on Victim's systems
- **Applying for credit cards -** require PII – may get leaked
- When logging in to online account, Victim must avoid to click on box that says "Remember password ?."
- *Hacking any app of Android phone cannot be done without installing hacking application on target phone*

Facebook hacking

- **Facebook hacking** : relatively difficult Hacking FB account requires years of programming knowledge & FB's infrastructure.
- Facebook Account hacking with Spyic
- **Spyic =** hack into Facebook accounts on target Android devices in 2 ways:
- **Hack Facebook with Keylogger utility**
- Spyic has inbuilt keylogger function.
- Records all keystrokes typed on target device. Next time Victim logs in FB account with password, hacker gets info

Spyic – features

- **100% discreet- Monitor remotely**
- **Spyic** = no signs of hacker's monitoring to victim
- Spyic = stealthy app. On both Android & iOS,
- Once installed it will run in background invisibly.
- App = very difficult to detect.
- Download size = 2 MBs.
- Spyic control panel **can be accessed** from any browser on Mobile phone / PC.
- **Spyic gives access** : call logs, contacts, messages, pictures, videos, notes
- **Cocospy :**
- Hacking of Facebook Account with Cocospy
- Cocospy = phone spy app for iOS & Android- stealthy

GMAIL hacking

- **Hacking : Gmail password with :**

✓ Pass Breaker

✓ TruthSpy:

✓ Victims **habit of auto-saving their Gmail passwords** on browser for easy access

- **Step 1: Type "chrome://settings/"**
- open web browser -Chrome.
- Type "*chrome://settings/*" in search column.
- **Step 2: Choose "Show Advanced Settings"**
- select option "Show Advanced Settings"- present in bottom. Tap on option - "Manage Saved Passwords".
- **Step 3: Tap "Show"**
- Hacker can see all accounts automatically logged in.
- From given list, choose Gmail account & tap "Show" in tab "Password".
- Password for Gmail account will be shown on screen

Hacking Gmail Account with Social Engineering

- If Hacker = friend or know victim , he can answer their security question.
- Hack their Gmail account via password recovery, choose - security question
- Display question that they have set for their account's security.
- If Hacker does not know answer, then search victim's social media profiles to guess

Thank you