Cyber Threat – Incidence Response Techniques (Module - 4 : DISSA Course)

Arijit Chakraborty

Feb 26, 2022

Password Grabbing

- Gmail hacker / attacker target a **particular low quality** website where victim is member & **hack their database** to get stored username & password of victim.
- Many victims **use same password** for Gmail & other purposes , eg xyzsuper.com
- Easy for Gmail hacker to get victim's password through low quality website xyzsuper.com

Cyber-attack :Ukraine : 2022

- Russian President Putin acknowledged existence of "patriotic" hackers,
- Moscow = widely thought to mastermind massive cyberattack on Ukraine's electricity network in December 2015.
- Feb 2022 = Websites of Ukrainian banks & government agencies disabled by DDOS attack after Russia attacked Ukraine- that Kyiv claimed were of Russian origin.
- Malware capable of erasing data found on hundreds of computers in Ukraine,

Targets – Power grid, BFSI, Hospitals, transport, stock exchange

Cyber-security experts at ESET & Symantec = **had recorded a second form of attack** on computer systems using a sophisticated "wiper" malware.

malicious software = showed timestamp of creation for 28 Dec 2021

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. -
- GST N , Ecommerce etc
- **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.***

Defending from cyber-threat
Internet Security

1. Access site which uses **https** (Hyper Text Transfer Protocol Secure) **-** performing Online transactions, Downloads etc,
2. If site **uses SSL/ TLS ,** verify Certificate details **-** Who is owner, Expiry date of certificate etc to confirm whether it is trusted
3. By clicking **lock icon.**
4. Scan downloaded files with **updated Anti-Virus Software** before using it.
5. Install & properly **configure a Software firewall**, to protect against malicious traffic.

Data security

1. Enable **Auto-updates of OS** & update it regularly.
2. Download **Anti-Virus Software** from Trusted Website & Install.
3. Ensure automatically **gets updated** with latest signatures.
4. Download **Anti-Spyware Software** from Trusted Website & Install, update

- 3. **Browser Security:**

1. Always update Web Browser with latest patches.
2. Use privacy or security settings which are inbuilt in browser.

4. Email security

- Use **strong password** for email account.
- Always use **Anti-Spyware & anti-virus Software** to scan emails for Spam.
- Remember to **empty Spam folder.**

Firewall

- Firewall = **software or hardware device** - examines data from several networks & either permits it or blocks it to communicate with user network
- Governed by predefined security guidelines. Defends from internal & external threats
- Supervises flow of traffic between distinctive parts of network.
- Firewall always exists between private network & Internet - filters packets coming in & out.

2 FA

- Google account settings & enable 2FA feature.
- Google Authenticator app to ensure no one else can access account without permission.

Zero Trust principle- Security Framework : 2021

- **“trust but verify” - Traditional security framework**
- Model became obsolete with cloud migration of business transformation initiatives & acceleration of a distributed work environment due to pandemic.
- Requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

CAPTCHA

- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) = type of security measure = **challenge-response authentication.**
- CAPTCHA helps protect from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account.

Deception technology: Honeypot

- network-attached system **set up as decoy to lure cyber attackers & detect, deflect , study hacking attempts**
- security mechanism = virtual trap to lure attackers

CERT-In Guidelines on Cyber-Security Audit

- Auditee and Auditing organizations needs to re-assess their risk profile and implement controls for minimizing the risk.
- Architecture changes, exposure of services, expanded organizational boundaries and changes caused = to be reviewed by Cyber Auditor
- Services exposed on adhoc and temporary basis (Pandemic) needs to be secured and properly audited. Such temporary changes to be reflected in BCP of organizations and thoroughly tested by Cyber / Forensic Auditor.
- Auditor & auditee organisation = ensure quality of audits should not be lowered in case of remote assessment = use of techniques : video calling for evidence verification, asking for snapshot of command output, online interview of process owner / suspect / witness etc
- Auditor = to maintain situational awareness & their assessments should also include tests derived from recent cyber-attacks trends

- Auditor to develop SOP for each type of audits and be clearly communicated to employees and auditee organization
- Periodic cybersecurity audits and audits when there is change in apps or infrastructure are critical & should not be avoided /diluted
- **Focus on ''External '' audit**

❑ Internal as well as external third-party audits are recommended for the cyber infrastructure of the organizations.

❑ To ensure independence and audits by domain experts, external audits should not be replaced by internal audits only.

- **SOP for Cyber / Forensic Audit engagement team**

❑ Employees deployed for audit should connect to centralized server of auditing firm and all audits related activity should only be conducted by connecting to the office network

❑ Auditors should only use office provided devices for conducting audits and these devices should only be used exclusively for audit activities.

❑ Auditing firms must follow CERT-In **Secure Data handling Guidelines**

❑ **Audit evidence / Data** should only reside at auditing Firm's servers at centralized location, NOT in auditee organisation server

Control gaps review & Audit Report

- Generate all security testing reports and recommendations.
- Suggest best possible patching and remediation for the identified vulnerabilities.
- Discuss & document the management action plan with timeline to implement the recommendations on the same
- In collaboration with client IT staff, resolve all the gaps identified in VAPT , and re-assess the vulnerability post closure of gaps
- Cyber security auditor = to submit recommendation, final audit report after the remedies/recommendations are implemented.
- The final report will certify the particular - Website “Certified for Security”.

Cyber Security Audit- ECGC

- **Purpose of Cyber security Audit**
- ECGC envisages review of processes & IT infrastructure with respect to :
- 1. Review based on IRDAI Circular Ref No: IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 (Guidelines on Information and Cyber Security for Insurers) amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020
- 2. ITGC (General Controls) Audit for IT systems handling Financial Information
- 3. Vulnerability Assessment and Penetration Testing of IT Systems
- The auditor shall also assist ECGC Ltd. in the following areas pertaining to IRDAI Circulars -
- 1. Adhering to changed or updated timelines of compliance
- 2. Adhering to further clarifications issued by IRDAI
- 3. Providing additional certification/s and clarifications as required by the IRDAI from the cyber security auditor