Lecture 4 - notes

1. Two-Factor Authentication (2FA) Recap

- Definition: Verifies identity using two distinct factors:
- Something you know (e.g. password)
- Something you have (e.g. phone)
- Something you are (e.g. fingerprint)
- Common Methods: SMS codes, TOTP apps, push notifications, hardware tokens, biometrics
- Risks: SIM swapping, phishing kits, user fatigue
- Best Practice: Prefer app/hardware-based 2FA over SMS

2. Malware Overview

- Definition: Malicious software designed to compromise confidentiality, integrity, or availability of systems.
- Categories:
- Propagation: Viruses, worms, trojans
- Payloads: System corruption, bots, spyware, phishing, rootkits

3. Malware Types

- Self-Replicating
- Virus: Needs host program and user execution
- Worm: Independent, self-propagating over networks
- Deception & Concealment
- Trojan Horse: Disguised as legitimate software
- Backdoor: Secret access bypassing security
- Rootkit: Hides presence and maintains privileged access
- Triggered Malice
- Logic Bomb: Activates under specific conditions
- System Compromise
- Exploit: Targets known vulnerabilities
- Keylogger: Records keystrokes
- Delivery & Installation
- Downloader: Installs other malware
- Auto-rooter: Gains root access remotely
- Virus Generator Kit: Creates custom malware
- Monetization & Tracking
- Spyware: Collects user data secretly
- Adware: Displays unwanted ads
- Denial of Service
- Flooder: Overloads systems
- Spammer: Sends bulk emails
- Platform-Agnostic

- Mobile Code: Executes across platforms (e.g. JavaScript, VBScript)

4. Malware Propagation Mechanisms

- Viruses: Infect executable content
- Worms: Exploit vulnerabilities, spread via email, file sharing, remote access
- Social Engineering: Phishing, trojans, spam

5. Advanced Persistent Threats (APT)

- Characteristics:
- Targeted, stealthy, long-term attacks
- Often state-sponsored or criminally organized
- Examples: Stuxnet, APT1, Aurora

6. Virus Details

- Structure: Infection mechanism, trigger, payload
- Phases: Dormant → Propagation → Triggering → Execution
- Targets: Boot sector, files, macros, multipartite
- Concealment: Encrypted, stealth, polymorphic, metamorphic

7. Worm Details

- Spread Methods: Email, file sharing, remote login
- Phases: Same as viruses
- Scanning Strategies: Random, hit list, topological, local subnet
- Progression: Exponential → Linear → Slow finish

8. Mobile Code & Drive-by Downloads

- Mobile Code: JavaScript, ActiveX, etc.
- Drive-by Downloads: Exploit browser vulnerabilities
- Variants: Watering-hole attacks, malvertising

9. Clickjacking

- Technique: UI manipulation to hijack clicks or keystrokes
- Tools: Transparent layers, iframes, stylesheets

10. Spam & Trojan Horses

- Spam: Bulk email, often malware carrier
- Trojan Horses: Hidden malicious code in useful programs

11. Malware Payloads

- System Corruption
- Data destruction, ransomware, BIOS attacks, industrial sabotage
- Attack Agent
- Botnet: Network of compromised systems
- Uses: DDoS, spamming, sniffing, keylogging, malware spreading

- Information Theft
- Keylogger, Spyware, Phishing, Spear-phishing
- Stealthing
- Backdoor: Secret access
- Rootkit: Hides malware, maintains control

12. Countermeasures

- Prevention
- Patch systems
- Access controls
- User awareness
- Threat Mitigation
- Detection
- Identification
- Removal
- Requirements
- Generality, timeliness, resiliency, transparency, minimal disruption

13. Antivirus Techniques

- Host-Based Scanners
- 1st Gen: Signature-based
- 2nd Gen: Heuristics, integrity checking
- 3rd Gen: Activity traps
- 4th Gen: Full-featured protection
- Behavior-Blocking Software
- Monitors real-time actions
- Blocks malicious behavior before damage

14. Perimeter Defences

- Ingress/Egress Monitors
- Worm Countermeasures:
- Signature filtering
- Payload classification
- Rate limiting/halting
- TRW scan detection

15. Distributed Monitoring

- Combines host and network sensors
- Central analysis and patch deployment