|  |
| --- |
| Essential elements of Cybersecurity: Visibility, Resilience, Identity threats, Data integrity, Risk acceptance, Prevention, Trusted apps infra, where spend time/money to protect  **Cybersecurity pillars**: Governance: Policy, Regulations/compliance, Standards, Norms/conventions, Audits, Procedures, Leadership, Knowledge mgmt., Oversight, Best practices like least privileges, 2-person integrity, n/w separation, Enclave), CISO: Security Policy, *Business Enablement*, Compliance, Protect Assets & Corp Secrets (CISO Type 1 [focused on compliance & doc; success by policy adherence]; CISO Type 2 [leans-in, address risk, collaborate w/ ops; success by buss ops]) | Security Systems Engineering **Network Segmentation**: Separation of n/w into mini-networks/segments w/ distinct security boundaries & protection profiles to limit ability to pivot from entry point . **Enclaving**: System resources that operate in the same security domain & share protection of a single, common, continuous security perimeter. Network Segmentation w/ independent (different) security profiles/controls “secure islands”| Tools development | OCO (project power by applying force), DCO (preserve the ability to protect data, n/w, systems), CooP (predetermined set of instructions on how org functions will sustain within 12 hrs. and up to 30 days on a disaster event) | Test & Evaluation | Chapter 1: Understanding Incident Response: Detect cyber incidents by *alert from security control* or *notification from an external (ISP or law enforcement) or a user alerts it (e.g., to helpdesk)*.  **Incident response process**: (never ad-hoc) *Preparation* (create IR plan, train team, acquire tools, prepping the env for defense & altering, practice/test) -> *Detection* (phase to 1st become aware of incident, > 100m events per day | human analysts have too much data to look at, Filter IoC from noise, SIEM tools loose effectiveness if heuristics not updated, **AI/ML tools** are better than humans at detecting incidents but take time to learn normal behavior | sources: system logs, ISP or law enforcement notif, internal users) -> *Analysis* (determine root cause, reconstruct actions of attacker from compromise to detection | Authz personnel from org or 3rd party, collect evidence: memory, log files, n/w connections, s/w processes, few hrs to many days, examine evidence: what happened , what affected, which systems, data leaks) -> *Containment* (Limit ability to continue compromising other n/w systems, conns to/from C2 infra, data exfil | Lock IP/Port on F/w, Remove n/w cable, stop bleeding) -> *Eradication & Recovery* (Remove attacker from impacted n/w, run anti-malware soln, wiped & reimaged, remove compromised user accts, apply patches, Recovery aligned with BCP/DR, reinstall fresh OS/apps, restore from backups, due-diligence: audit existing user & admin accounts, a full vuln scan) -> *Post-Incident Activity* (Full review of incident & actions taken with stakeholders, retrospective (+ve & -ve), written report w/ chain of events, root cause, Avoid jargon [People outside IT read it, explain technical jargons, comply w/ regulatory & statutory req]) | Role of digital forensics: None in DoS attack, but in C2 data exfil | IR performs vuln scan and remediation OR limiting exploitation of attacker OR managing personnel, whereas DF doesn’t do those.| Alert fatigue: Thousands of alerts from tools leading to overwhelming (false positives) and miss important ones (delayed response). | **Incident response framework**: components of IR capability: *personnel, policies, procedures* | **IR charter**: A document w/ sr. leadership support, define constituency (CSIRT responsibilities, separate by domains or by org name for large orgs), mission statement (mission creep can occur by expansion of responsibilities, counter it with mission statement), service delivery (defined list of services | **proactive** [training, emerging threats, test & deploy of tools like EDR] & **reactive**[respond to incidents, entire IR process w/ forensics]) | Benefit of IR charter is to socialize CSIRT (**Org’s 911 force**) to bring transparency to employees. **CSIRT roles** (CERT is for US-CERT or CERT/CC for Carnegie Mellon): **CORE (full-time IR):** *IR coordinator*: CSO, CISO, ISSO | *CSIRT sr. analysts*: trained & experienced IR, DF, n/w data examination | *CSIRT analysts*: less experience in IR | *SOC analyst*: 24/7 SOC monitoring, contact for detection and alerts [in-house SOC or outsourced / SOCaaS] | *IT security engineers/analysts*: Deploy/maintain/monitor security s/w or h/w, part of preparation process of IR, Ensure security apps (AV) & devices (f/w, SIEM) configured to alert incidents & to log events | **TECH SUPPORT**: not CSIRT; can access systems/processes affected by incident (n/w & server admin, app support, desktop support, helpdesk) | **ORG SUPPORT**: Legal, HR, Marketing/Comms, Facilities, CorpSec | External: HTCIA [High Tech Crime Investigation Association] (international professionals & students), InfraGard (in US by FBI), Law enforcement, Vendors. **Incident response plan**: **Document** that outlines high-level structure of org’s IR capability | Annual review | IR Plan includes: *IR charter (mission stmt & constituency), Expanded services catalog (details of forensic services like evidence recovery, memory forensics, reverse engg), CSIRT personnel (roles & resp), Contact list, Internal comm plan, Training (frequency, CSIRT tabletop exercise once per year), Maintenance* | **Incident Classification**: High (significant damage, corruption, loss of critical data, wide-spread systems like n/w intrusion, physical compromise, critical info leak, loss of confidential info, widespread/growing malware > 25% hosts, targeted attacks on IT infra, phishing attacks on domain/brand), Medium (DoS, Misuse of authz access, Automated intrusion, confined malware infection, Unusual system perf, Install of malicious s/w, suspicious changes, playbooks), Low (policy violations, lost or stolen laptop or mobile w/ confidential info, install unauthz s/w, malware on one computer.);  **Incident response playbook**: Part of IR plan | Set of instructions/actions to perform during IR | Not checklists but flowcharts | Guide for IR | **Escalation procedures**: Part of IR plan | Who decides to create incident based on anomalies found.| **Testing IR framework**: High-level incident scenario w/ entire team & one playbook -> report on table-top exercise forwarded to sr. mgmt. |
| Chapter 2: Managing Cyber Incidents: Engaging the incident response team: CSIRT models: ***SOC escalation*** (initial detection + investigation, has access to IPS/IDS & AV, can be a 3rd party MSSP: Managed Sec Srv Provider) Steps to escalate: Alert is received by Tier-1 SOC analyst -> decides it as incident or not -> performs initial investigation -> Escalate to SOC manager -> escalates to CSIRT to address incident. **Issues**: 1. Several individuals handling incident before CSIRT is engaged. 2. More time to address incident by CSIRT when escalation by SOC not properly documented. 3. Tier-1 people to be trained in identifying incidents from events. 4. Comm gaps between SOC and CSIRT delay IR. | ***SOC & CSIRT combined***: SOC under CSIRT org, Faster incident completion w/ high precision. Only for in-house SOC & Not for orgs with NOC, Needs more CSIRT managers. | **CSIRT fusion center** (expensive, needs full-time threat intel analysts); War room: Location for CSIRT to manage incident, can be dedicated room for high # incidents or reuse meeting room for low incidents; workspaces, team displays, note sharing, whiteboards, restricted access (prevent info leak) | **Communication** | **Staff rotation**: *Incident commander (IC)* defines shifts for IR people. 24hrs after incident or when incident is contained. | **Incorporating crisis communications**: GDPR Article 33 -> (72-hr breach notification req. to data protection authority; details on breach & impact; rapid IR & accurate breach doc), HIPPA Rule 45 CFR 164.400-414 -> by 60 calendar days notification data breach, DFARS 252.204.7012 (Defense Fed Acq Rules Supplement) -> instant report to DoD | Internal, External, Public. | **Investigating incidents**: *Scope*: Entire n/w -> Systems impacted w/ attack. Find “patient zero” (1st system compromised). | *Impact*: CIA analysis. | *Root-cause*: Not a simple vuln, often seq of events. | *Attribution*: Who attacked? | **Incorporating containment strategies**: Physical (cable removed) | Network (switches) | Perimeter (Firewall) | Virtual (Hypervisors, SDI (infra), SDN, IaC, Serverless) | **Getting back to normal: eradication and recovery**: Cannot be 100% sure malware is removed | must reimaging w/ good backup | 3 VLANs: Infected/staging/prod | Recovery: Cyber hygiene check (patches), Update alert profile (IDS/IPS), Changes review (Temp or Perm), Vuln scan (Scan & Remediate), After action report (IoC). |
| Chapter 3: Fundamentals of Digital Forensics: Putting scientific principles to legal | **Legal aspects**: Laws & Regulations (Title 18 US Code Section: 1029: Fraud & related activity in conn w/ access devices, 18 USC 1030: (1986) **Computer Fraud & Abuse Act** (CFAA), IR: DoS for example (Unauthz access & damage to PC; require legal authz to access PC during investigation; civil+criminal penalties for violations), Electronic Comm Privacy Act (ECPA): Unauthz interception of comm via electronic means [telco & internet] & CALEA: Comm Assistance for Law Enforcement Act: ISPs to authz n/w to law enforcement agencies for surveillance, Economic Espionage Act of 1996 (EEA): 18 USC 1831-1839, theft of trade secrets a crime, Riley v. California (2014): Warrantless search/seizure of digital contents of mobile during arrest is unconstitutional, Carpenter vs. US (2017): Law enforcement can seize cell phone with valid warrant.) | **Rules of evidence**: Rule 402 (Test for relevant evidence): evidence must be admissible & prove or disapprove facet of case | 502 (Attorney-Client Privilege and Work Product): Reports contain actions taken + info obtained; Discussion b/w client-attorney not admissible in court | 702 (Testimony by Expert Witness): CSIRT/SOC analyst may be allowed to testify as an expert witness | 902 (Evidence that is self-authenticating): Verification of **digital evidence integrity thru hashing** | 1002 (Best evidence rule): original writing, recordings or pics can be evidence | 1003 (Admissibility of duplicates): critical step of forensics is to make copy of image/media; Analyst have to testify to have performed correctly. | **Digital forensics**: History: FBI created CART (Comp Analysis & Response Team), CERT Coordination Center (CERT/CC), International Organization on Computer Evidence (IOCE), Scientific Working Group on Digital Evidence (SWGDE), Regional Computer Forensic Laboratory (RCFL). | **DF process**: DF Research Workshop (DFRWS) digital investigation framework: Identification: **Locard's exchange principle:** 2 objects contact leave a trace behind; Trace evidence: Logs, Cookies, PCAP, Memory, Deleted files, Timestamps, Packet Header info, RFID tracking devices, CCTV, voice, pictures | Preservation: safeguard from modification & deletion; Secure backup, controls for Log file remove/modify, Isolate system (physical, logical, NAC, perimeter controls), users should not access suspect system, VMs/IaC/SDx: Snapshots | Collection: Begin acquiring digital evidence; Volatile evidence is lost when system powered off; For n/w equipment, it is active conns or log data stored on device; For PCs, it is memory or ARP cache; IETF Guideline for evidence collection & archiving (RFC 3227) has **order of volatility**: *Registers & cache* -> Routing table / ARP cache / process table / RAM -> Temp filesystem -> Disk -> Remote log / monitor data -> Physical config / n/w topology -> Archival media; External hard-drive is non-volatile. **Evidence handling**: Do not alter original evidence, Every action taken must be documented, **Chain of custody**: evidence collected, preserved, transferred, analyzed (electronic or pen-paper, NIST has template [Electronic-media: Item-Number, Desc, Manufacturer, Model, Serial number] [Log files or images: Date/time acquired, Desc, Method, Storage drive, File/image name, Hash] Other details in template: Tracking No, Date/time, FROM/TO, Reason) | Examination: Forensic tools & techniques to extract data (memory images, desktop images, log files, network captures) on copy of backup | Analysis: Correlate the data obtain from evidence with data info on network | Presentation: Reporting needs to be clear, concise, unbiased; May require court testimony (opinions + conclusions of analyst) | **Digital forensic lab:** Physical security | **Tools** [**hardware** (min 32GB RAM, 2TB of storage, separate computers with & without internet, **physical write blocker** to stop writing data to evidence drive); A dedicated forensic imaging station is possible but expensive; high-capacity USB drives needed (at least 6); Two hard-sided cases needed for shipping (hardrives & laptops); | **software:** Autopsy: [open-source | automates | Timeline analysis | Hash filtering | Keyword search | Web artifacts: History, bookmarks, cookies from 3 browsers | Data carving (deleted files) | Multimedia (exif from pics)], TSK (The Sleuth Kit): [opensource | cmd line tools | Library | Functions: *[Volume & File system analysis, Download, Documents, History, Licenses]*], EnCase: [OpenText | full-spectrum gold-standard PC/Linux/Mac | Apple T2 security chip bypass | smartphones & tablets >27000 mobile device profiles | AI powered | OS decryption | cloud connection | easy report | in Gov, Law Enf | Expensive | E01 format images], Forensic Toolkit (FTK): [Gov & Law Enf | Alternative to EnCase], X-Ways forensics: [German, Low-cost (1300$/year/seat) w/o n/w-access or remote capture), Runs from USB , Win XP/2003/Vista/7/8/8.1/2012/10/2016], Volatility: [Looks at RAM & other volatile storage; FOSS; Win/Linux/Mac; Annual contests to build plugins], Registry Recon: [Windows Registry only; deleted registry can be accessed even if reimage by IT; subscription based pricing: month, year, 5 year] | **Linux forensics tools**: DEFT Zero (Digital Evidence & Forensic Toolkit): FOSS; GNU, Booted from USB or CD, *Ensures integrity* | Paladin: Live-Linux, Ubuntu, malware analysis, hashing, imaging; Run from USB; Triage/Search/Image | SIFT (SANS Investigative Forensic Toolkit): Comprehensive, Ubuntu, imaging, memory analysis, timeline creation, FREE, On Windows with WSL | CAINE (Computer Aided Investigative Env): FOSS; GBU; Italy; GUI (w/ Autopsy, bitlocker, Volatility plugins) | LiFTeR (Linux Forensic Tools Repository): Fedora, RedHat, by Carnegie Uni SEI | REMux: Malware reverse engineering tools, Ubuntu, Analyze Windows & Linux]; **NIST provided guidance on testing forensic tools thru CFTT (Computer Forensic Tool Testing) |** Jump Kits: (Portable) Forensic performed at onsite use preconfigured kits w/ h/w & s/w to store & analyze evidence | **Contain** Forensic laptop, n/w cables, Physical write blocker, External USB drives, USB devices, Bootable USB/CD, Evidence bags/boxes, Anti-static bags, Chain-of-custody forms, Toolkit, notepad & writing instrument; pre-staging jump-kits at key locations will reduce response time for large orgs. |
| Chapter 4: Collecting Network Evidence: Capturing n/w traffic is invasion of privacy if no policy states n/w monitoring takes place. Employees understand use of systems being monitored; N/w diagram: Allows for quick identification of evidence sources; **OSI model**: Media layers (Physical [bit/symbol], Data-link [frame], Network [packet]) & Host layers (Transport [segment/datagram], Session [data], Presentation [data], Application [data]) | Switches (connect PCs), Routers (connect networks), Firewalls (web filter, DLP, logs on allow/deny traffic), NIDS/NIPS (malicious activity on n/w infra) [**conn logs** (src ip, dst ip, protocol), **remote access logs** (F/w is VPN concentrator for remote access, connected systems & time)], Web proxy (URLs, history of C2 connections for weeks/months; useful for reconstructing attack)], Domain controllers (authn servers, credential manipulation / uses), DHCP server (dhcp logs), App servers (SMTP logs) | Preparation | Network diagram | Config; **NetFlow** (monitor traffic across n/w; deep insights into internal traffic of systems) [**East-West Traffic** (lateral movement within single n/w segment) & North-South Traffic (from one n/w to other; traverse routers)] | MAAS (Metal-as-a-Service): Facilitate & automate deployment of hyperscale computing env (big data & cloud). | Network tap: in-line conn that detects/inspects packets as they flow within a segment | **tcpdump** packet capture: (from memory to file): **WinDump** (tcpdump on Windows); **WinPcap** (Packet capture on Windows, to be installed on every windows), **RawCap** (alternative to WinPcap, without the need to install on every Win host, can run from USB drive) | Record the evidence captured: File Name (std naming convention), Desc, Location (IP or host desc), Date/time (transferred to medium), MD5 hash. | **Cellebrite UFED**: Forensics for mobile devices; Bypass patterns, password, PIN and overcome encryption on Android & iOS; Collect data from phones, drones, SIM cards, SD cards, GPS devices; Access to 40+ apps on Android; h/w and s/w packets available | **Wireshark packet capture**: GUI or TTY-mode (Tshark); Multi-platform; can run from USB; Free & OpenSource Forensics tool; Deep inspection of hundreds of protocols; Live & offline capture; Rich VoIP analysis; Output can be XML, PostScript, CSV, plain text; |
| Chapter 5: Collect Host-Based Evidence: CPU registers->RAM->PageFile or Swap File->Storage drives: SDD/HDD/USB drives | **Volatility**: How data is maintained after logoff or shutdown. Options for acquiring evidence: Local or Remote | **Live acquisition**: When system is ON | **Offline acquisition**: dead-box forensics; used by law enforcement; powered OFF & drive removed *Benefits of offline*: Works on systems no longer functional; *Drawbacks of offline*: special tools to acquire drive evidence; Loss of volatile memory; time-consuming; **Memory dumps contain**: Passwords to encrypted volumes (TrueCrypt, BitLocker, PGP Disk), account login credentials for webmail and social network services. | Collection procedures: **Acquiring volatile memory**: **Local**: Run from USB tools [**FTK Imager** (Windows; running memory of system; good for dead-box forensics; fast due to distributed processing engines; visualizations for relationships & patterns), **WinPmem** (Opensource; Windows; XP, 10, 3 methods to create dumps, output format:raw or AFF4), **RAM capturer** (live system; opensource; Windows; run from USB; works when anti-debug or anti-memory dump is in place)] with two partitions (one for tools, one for data captured) | **Remote** (Not possible when system is offline) [WinPmem (NetCat, RDP or PsExec), Virtual machines: (VMWare stored volatile memory in **VMEM** file; Snapshots in **VMSN** file; Transfer VMSS & VMEM files to USB or n/w share;)] | **Acquiring non-volatile evidence**: Registry keys, Event logs. Tool: **CyLR.exe** (open-source, can run from usb or system, can send data to remote) | Checking for encryption (FDE) | Tools to check: Endpoint Disk Detector from magnet forensics; **Incident Isolation**: Enclaving (segments with different security profiles/controls), Network Segmentation (divide into small subnets); | **Digital Forensic tools**: **Hardware** [Disk imager/duplicator (Tableau HDD duplicator: Image SATA, Disk-to-file, Format/Wipe, Hash (MD5/SHA1), Blank disk check) (ATRIO: All-in-one hardware/software; parallel processing capability; AI-based object detection; Rugged, durable casing, NIST-accredited) (FRED: Multiple drives simultaneously, sequentially, high availability heat sink, power, multiple RAID, RAM/CPU optimized for forensics software), network scanner, PC/Linux with many I/O ports, hard drives], **Software** [Network scanner/sniffer, Data analysis, regedit analysis, Deep packet inspection, UEBA (User Entity Behavior Analysis): Heuristics & AI/ML tools] |
| Chapter 6: Forensic Imaging: Forensics imaging ≠ Copying files or Cloning; Imaging captures entire drive: Slack space, Unallocated space, possible access to deleted files, metadata of volume | **Cloning** created 1-to-1 copy of drive resulting in fully functional/bootable drive: can be cumbersome for dead-box forensics, includes master boot record, Full disk enc makes clone difficult to analyze | **Imaging** copies all files but is not intended to create a bootable/usable drive: easier for forensic to analyze & does not require master boot record. **Types of imaging**: Logical, Physical, Dead, Live. | **Logical image** of a particular drive (e.g. D drive) allows analyst to copy only suspected portion, not include full disk enc protections, and accelerate the process. Drawbacks: Not bootable; Loss of chain of evidence – too many questions/reasonable doubt. And does not capture unallocated space on physical drive or any data not part of the file system (e.g., deleted files, trace data). **Understanding digital imaging**: **Raw images**: (.dd) bit-for-bit copy; lacks compression & metadata | **EnCase evidence files**: (E01) Includes image metadata (type, os, timestamp), CRC for file integrity of blocks copied, preferred output for law enforcement & legal as it ensures integrity w/ compression.|**AFF4** (Adv Forensics File Format) | **AD1** (AccessData Evidence file) | Delete: Hide from OS, OS overrides only when you want space for other files; Wipe/Erase: Permanent, override with 0,1; Shred: Wipe/erase for 1 file;  **Imaging tools**: FTK Imager (logical & physical volumes, memory, output in multiple formats; runs on removable media) | EnCase Imager | AFF4 Imager: CLI, isolate based on time & volumes to reduce time-to-image| dd: Linux cmd to clone whole drives or partition| Virtualization tools: Entire OS env in s/w; pause VM, create copy of VM & state files; **Write blockers**: Software write blockers (sits between OS & evidence; ensure there is read-only access to evidence) | Hardware write blockers (physical piece sits between evidence drive & system performing acquisition, allows one-way data transfer f/ disk to evidence analysis system [data diode]); | **Imaging techniques**: ***Dead imaging*** (media not energized; most comprehensive for evidence collection; complete preservation & analysis of physical volume; uses h/w write blocker for integrity) | ***Live imaging***: when system running due to criticality, run imaging from usb, w/o changing ops| ***Remote Memory Acquisition***: not preferred unless direct approach fails; Tools for remote imaging: **WinPmem** & **F-Response** (no install on target host)| Virtual machines, Linux imaging) | **Analyzing evidence steps**: Understand domain/env/usecase -> Break evidence into structures -> discover patterns -> connect dots to show what happened on suspect system; |
| **preparation phase in IR process | effective IR plan | contribute to reducing the impact of future cyber incidents?** [A] The preparation phase is vital in the incident response process as it establishes the groundwork for effective incident management through risk assessment, resource allocation, and the development of clear policies and procedures. Key elements of an effective incident response plan include defining the incident response team structure, establishing incident classification criteria, outlining detection and analysis procedures, and detailing containment and recovery steps. This phase enhances organizational readiness by conducting training and simulations, which ultimately reduces the impact of future cyber incidents by ensuring swift, coordinated responses, minimizing downtime, and preserving critical assets. |
| **Electronic Communications Privacy Act (ECPA) | affects evidence in forensic investigation | steps to comply w/ legal standards while collecting data?** [A] The Electronic Communications Privacy Act (ECPA) plays a crucial role in regulating the interception and collection of electronic communications, impacting how investigators gather network-based evidence during forensic investigations. Under the ECPA, unauthorized interception of electronic communications, such as emails or network traffic, is prohibited unless certain legal standards are met. To comply with this law, investigators must obtain proper authorization, such as a warrant or consent from the involved parties, before collecting any data. Additionally, they should implement clear documentation processes to demonstrate compliance with legal standards, ensure that only relevant data is collected to minimize privacy intrusions, and maintain transparency throughout the investigation to uphold the integrity of the evidence. By following these steps, investigators can navigate legal boundaries effectively while conducting thorough forensic analyses. |
| **Describe how evidence is captured at different layers of the OSI model during a network forensic investigation. What type of evidence is typically collected at the Network Layer and Application Layer, and how do these artifacts contribute to reconstructing a cyberattack?** [A] During a network forensic investigation, evidence is captured at different layers of the OSI model, providing unique insights into network activities: 1. Data Link Layer (Layer 2): Evidence includes Ethernet frames and MAC addresses, which help track devices and communication patterns on the network. 2. Network Layer (Layer 3): Evidence consists of IP packets, including source and destination IP addresses and routing information. This data reveals the paths taken by packets, helping identify unauthorized access or lateral movements. 3. Transport Layer (Layer 4): Collects TCP/UDP segments and port numbers, crucial for analyzing host connections and session establishment.  4. Application Layer (Layer 7): Captures application-level protocols like HTTP, including request/response headers and URL logs. This information helps identify user activities and potential data exfiltration. Together, artifacts from the Network Layer and Application Layer contribute to reconstructing a cyberattack by detailing the network paths used and the specific actions taken by attackers, enabling a comprehensive understanding of the attack and its impact. |
| **Discuss the role of hashing in ensuring the integrity of digital evidence. How do tools like MD5 and SHA-1 verify that forensic images have not been altered? What are the potential risks of using hash algorithms, and how can investigators mitigate these risks?** [A] Hashing is essential for ensuring the integrity of digital evidence by generating a unique hash value for data, which acts as a fingerprint. Tools like MD5 and SHA-1 compute hash values for forensic images, allowing investigators to verify that the evidence has not been altered by comparing the original hash with a recalculated hash after handling the evidence. However, MD5 and SHA-1 are vulnerable to collisions, which can undermine integrity checks. To mitigate these risks, investigators should use stronger algorithms like SHA-256 and implement multiple hashing methods, ensuring thorough documentation of the hashing process for transparency and reliability. |
| **Organizations classify incidents into categories based on severity (high, medium, low). Describe the factors that determine the classification of an incident. Provide an example of a high-severity incident and explain the steps that would be taken to respond to it under an organization's incident response framework.** [A] Organizations classify incidents into categories based on factors such as impact, scope, urgency, and type of incident. A high-severity incident example is a data breach involving the unauthorized access of sensitive customer data. In response, the steps taken would include detecting and analyzing the breach, containing it by isolating affected systems, eradicating the threat by removing malware, recovering systems from clean backups, and conducting post-incident activities to review and improve response plans. |
| **With the increasing adoption of cloud services, digital forensics faces new challenges. Explain the unique difficulties associated with collecting and preserving evidence in a cloud environment. How do investigators ensure the chain of custody when dealing with cloud-based evidence?** [A] Collecting and preserving evidence in a cloud environment presents challenges such as data ownership, access controls, and multi-tenancy, which complicate direct access to evidence. Additionally, the ephemeral nature of cloud resources can lead to data loss. To ensure the chain of custody with cloud-based evidence, investigators should maintain detailed documentation of all actions taken, including access requests, timestamps, and communication with cloud service providers. They should also utilize cloud-specific forensic tools that support the preservation of data integrity and compliance with legal standards during the collection process. |
| **Artificial Intelligence (AI) and Machine Learning (ML) tools are increasingly being used in digital forensics. Discuss the benefits and limitations of AI-based forensic tools, particularly in analyzing large datasets. What ethical considerations should be taken into account when using AI in forensic investigations?** [A] AI and ML tools in digital forensics offer benefits such as enhanced data analysis speed, improved pattern recognition, and the ability to process large datasets efficiently, enabling faster identification of anomalies and potential threats. However, limitations include potential bias in algorithms, reliance on quality of training data, and the risk of overfitting results. Ethical considerations include ensuring transparency in AI decision-making, safeguarding privacy rights, and avoiding discrimination in the analysis process. It is crucial to validate AI findings with human oversight to maintain the integrity of forensic investigations. |
| **Cross-border cybercrime investigations can be complex due to differences in national laws and jurisdictions. How should a forensic investigator approach a situation where evidence spans multiple countries? What international laws and agreements, such as the Budapest Convention, guide investigators in handling cross-border digital evidence?** [A] When dealing with cross-border cybercrime investigations, forensic investigators should approach the situation by understanding the legal frameworks of each jurisdiction involved and seeking proper legal authority to collect evidence. They should collaborate with local law enforcement and international agencies to navigate jurisdictional challenges. The Budapest Convention provides guidelines for cooperation among countries on cybercrime, establishing standards for the exchange of information and mutual legal assistance. Additionally, investigators should be aware of data protection laws, such as the GDPR, which may impact the handling of personal data during the investigation. |
| **In many cases, forensic investigators are called to provide expert testimony in court. Describe the key components of a forensic report that would be presented in court. What strategies should an investigator use to communicate technical findings clearly to non-technical audiences, such as judges and juries?** [A] A forensic report presented in court should include key components such as an executive summary, detailed methodology, findings, evidence analysis, chain of custody documentation, and conclusions. To communicate technical findings clearly to non-technical audiences, investigators should use simple language, avoid jargon, employ visual aids (like charts and diagrams), and provide real-world analogies to explain complex concepts. Additionally, practicing clear and concise explanations while anticipating questions can enhance understanding and retention of information by judges and juries. |
| **Acquiring volatile memory from a live system | FTK Imager and WinPmem | challenges capturing volatile memory from VMs?** [A] Acquiring volatile memory from a live system can be performed using various tools, with **FTK Imager** and **WinPmem** being two notable options. **FTK Imager** is a versatile tool that not only allows for memory acquisition but also provides capabilities for creating forensic images of storage devices. It is particularly effective in environments where a graphical user interface is advantageous, making it user-friendly for analysts. FTK Imager can be used in scenarios where a comprehensive analysis is required, as it allows for simultaneous imaging of physical drives while capturing memory. **WinPmem**, on the other hand, is a command-line tool specifically designed for acquiring memory from Windows systems. It is lightweight and can operate in environments with limited resources, making it effective in situations where minimal impact on the system is desired. WinPmem is particularly useful for capturing memory in live systems where speed is critical, as it can quickly dump the contents of RAM.  When capturing volatile memory from virtual machines, challenges arise due to the complexities of virtualization environments. Memory acquisition must consider the hypervisor layer, as direct access to the virtual machine’s memory might not be straightforward. Tools like FTK Imager may not natively support virtual environments without additional steps, such as using snapshot functionality. Moreover, virtual machines can encapsulate multiple instances of volatile memory, necessitating careful identification of the correct instance to capture. Additionally, the performance overhead of capturing memory from virtual machines can lead to latency, which may affect the state of the VM and the data being collected. Thus, while both FTK Imager and WinPmem are valuable tools, the choice depends on the specific context of the investigation and the operational environment. |
| **Discuss the role of the CISO in an organization. How does a "Type 1" CISO differ from a "Type 2" CISO in terms of security strategy and business enablement?** [A] The Chief Information Security Officer (CISO) is responsible for overseeing an organization’s security strategy and policies. A Type 1 CISO focuses heavily on compliance and documentation to prevent liability during a breach, with success measured by adherence to security policies. On the other hand, a Type 2 CISO collaborates with operations teams and focuses on addressing risks to enable business operations, prioritizing security as a facilitator of the business mission. |
| **Explain the steps involved in the post-incident activity phase of an incident response process. Why is this phase critical to improving future incident handling capabilities?** [A] The Post-Incident Activity phase involves a thorough review of the incident, a retrospective analysis of what worked and what didn’t, and the creation of a written report detailing the root cause and the actions taken. This phase is critical as it identifies lessons learned, improves the organization’s response to future incidents, and ensures compliance with regulatory and legal requirements. |
| **Describe how network segmentation and enclaving help contain incidents and limit the spread of malware within a network. Provide real-world examples of each approach.** [A] Network segmentation divides the network into smaller, isolated segments, reducing an attacker’s ability to move laterally across the network. For example, separating the accounting department from the rest of the network limits the spread of malware if a compromise occurs. Enclaving creates secure "islands" within the network, each with its own security controls. This approach is often used in high-security environments, like military systems, to ensure that a breach in one enclave does not affect others. |
| **What are the legal and ethical implications of using offensive cyber operations (OCO) in the context of cybersecurity forensics? How do organizations balance these activities with the need to protect privacy and civil liberties?** [A] Offensive Cyber Operations (OCO) involve actively disrupting or degrading an adversary’s systems, which raises significant legal and ethical concerns, particularly around privacy, sovereignty, and the potential for collateral damage. Organizations must ensure that OCO activities comply with laws like the CFAA and international agreements. Balancing these operations with privacy rights requires strict oversight, clear policies, and legal authorizations to prevent abuses. |
| **In a digital forensics investigation, why is it critical to ensure that the integrity of the evidence is maintained throughout the collection, preservation, and analysis phases? What tools and techniques are commonly used to verify the integrity of forensic evidence?** [A] Maintaining evidence integrity is crucial to ensure that the evidence is admissible in court and has not been altered or tampered with. Techniques like hashing (using MD5 or SHA-1) are used to verify the integrity of forensic images, ensuring that the data collected remains unchanged. Write blockers prevent modification to the evidence during analysis, and chain of custody documentation tracks every action taken with the evidence, preserving its legal admissibility. |