Unit 1 Notes

Introduction to Incident Response : windows sysutilities
sysmon

Reference: Slides - Dr. Dharmesh Dave.

Defn: Incident is an occurrence of an action or situation that is a seperate unit of experience.

Defn: Computer software is a programming code executed on a computer processor. The code can be machine-level code or code written for an operating system.

* Trojans are leading form of malware on Android

Defn: Information warfare can be a combination of lies, manipulated truths, manufactured media, or in some cases exploiting human nature to sow confusion. Information warfare is a battle fought in cyberspace over networks.

Defn: Information Security (InfoSec) covers the tools and processes that organizations use to protect information.

* 3 pillars of InfoSec - CIA Triad.

Vector, scarf, payload
BLL

Def^{n}: A MITM attack involves an attacker to intercept the network thereby compromising it.

Def^{n}: A DOS Attack attempts to knock a network/service offline by flooding it with traffic to the point the network/service can't cope.

Def^{n}: A DDOS Attack hijacks devices using botnets to send traffic from multiple sources to take down a network.

Def^{n}: Phishing involves the hacker sending an email designed to look like it has been sent from a trusted company or website. Spear Phishing on the other hand has a specific target.

Def^{n}: A Cross-site Scripting (XSS) attack attempts to inject malicious scripts into websites or web apps.

Process: Logging, Categorization, Prioritization, Assignment, Task Management, SLA Management, Resolution, (Closure).

Dynamic Link Libraries (DLL)

DLL is a file that contains reusable code and data that can be used by multiple programs at the same time. DLLs are commonly used in various types of software applications, including OS, device drivers, plugins, libraries.

- An attack vector is a method of gaining unauthorized access to a network or computer system.
- An attack surface is the sum of all attack vectors on a digital surface.

→ compromised credentials, weak credentials, insider threats, missing/poor encryption, misconfiguration, ransomware, phishing, vulnerabilities, brute force, DDOS, SQLi, Trojans, XSS, session hijacking, MITM, third & fourth party vendors.

→ Password Requirements, Always-on software, Distributed Infrastructure.

Payloads

A piece of malicious code that is used to execute a specific action on a target system.

- The vulnerability in a flash player is what is exploited to deliver the payload. How the payload is delivered is the attack vector, which is, the webpage ??

→ challenges in Log Management :

1) variety (standardization)
2) volume (Load Balancer)
3) velocity

→ Incident Response Plan - compromised data, roadmap for implementing IR capability, formal | focussed | coordinated

1) Mission
2) Strategies & goals
3) senior Mgmt Approval
4) Org. approach to IRM
5) How IR Team will communicate
6) Metrics for IR effectiveness
7) Roadmap
8) How the program fits?

Reference: Estimating Cost of an Incident

1) Cost to the business
2) Cost of providing services to resolve the incident

Cost To The Business :

- happen frequently
- have significant business impact
- affect groups of users we can more easily identify

} why?

- assessing loss production hours
- assessing loss to profitability
- assessing damage to reputation

} How?

Defn : Cost Code, as used by many organizations, are cost brackets to identify the cost of an incident. It is a way of approximating the actual cost of an incident.

Cost of Incident Management :

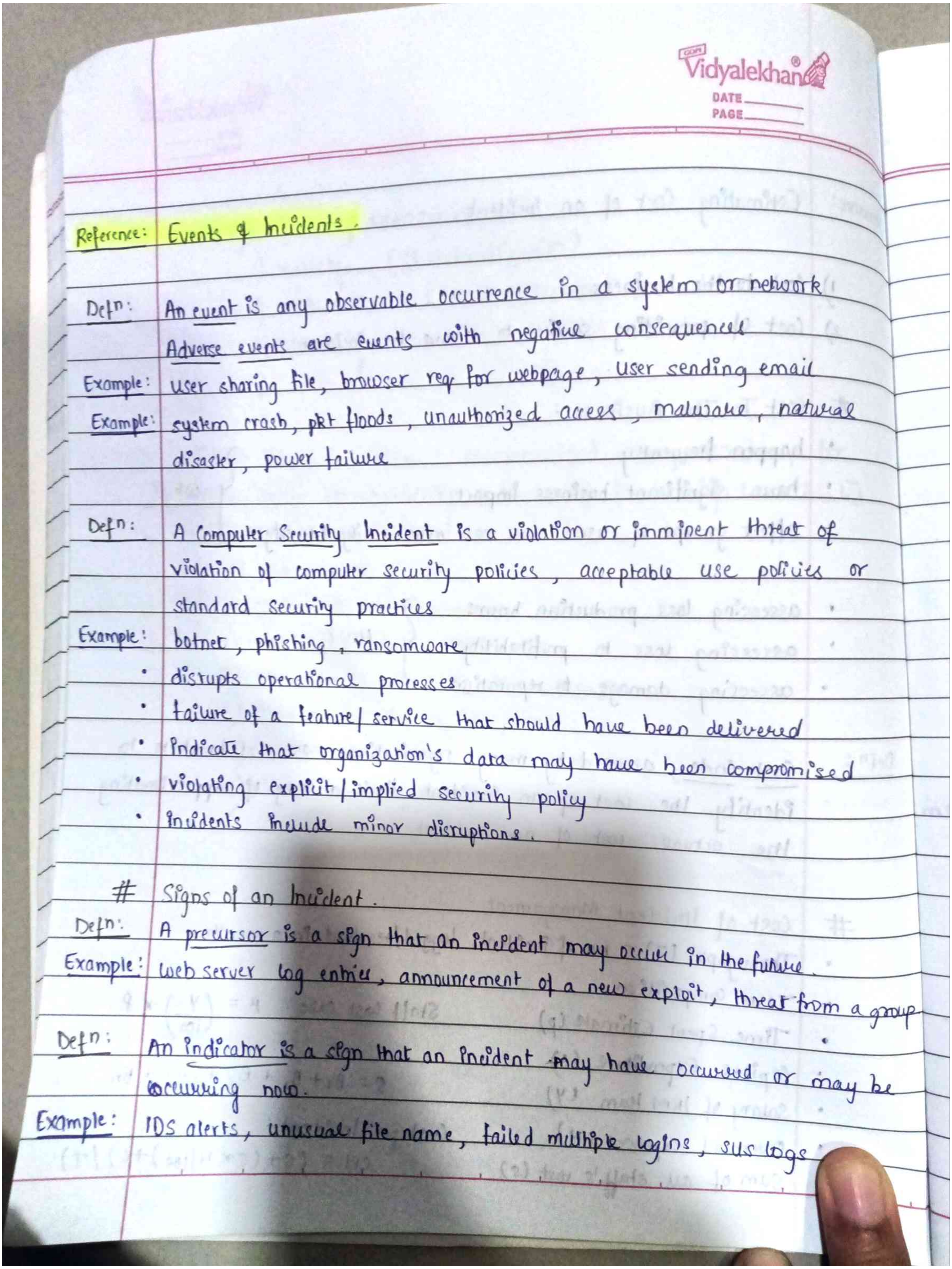
- Throughput (T) - no. of incidents logged/resolved in a month.
- Team Composition
- Time Spent Estimate (p)
- Capital Expenditure (C)
- Salary of IRM team (Y)
- Overhead expenses (H)
- Sum of all staff's cost (S)

Staff Cost Calc : $B = \left(\frac{Y}{100}\right) * P$

$S = B_1 + B_2 + B_3 + \dots + B_n$

Cost per Incident :

CPI = $(S + (S * H/100) + C)/T)$



Reference: Events & Incidents.

Defn: An event is any observable occurrence in a system or network
Adverse events are events with negative consequences

Example: user sharing file, browser req for webpage, user sending email

Example: system crash, pkt floods, unauthorized access, malware, natural disaster, power failure

Defn: A Computer Security Incident is a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices

Example: botnet, phishing, ransomware

- disrupts operational processes
- failure of a feature/ service that should have been delivered
- indicate that organization's data may have been compromised
- violating explicit / implied security policy
- incidents include minor disruptions.

Signs of an Incident.

Defn: A precursor is a sign that an incident may occur in the future.

Example: web server log entries, announcement of a new exploit, threat from a group

Defn: An indicator is a sign that an incident may have occurred or may be occurring now.

Example: IDS alerts, unusual file name, failed multiple logins, sus logs

Categories of an Incident:

1) High – data theft, identity theft, unauthorized access
- impact on large number of systems/people
- potential large financial risk or legal liability
- threatens confidential data
- adversely impacts an enterprise system or service critical to the operation of a major portion of the organization.
- poses a significant & immediate threat to human safety
- high probability of propogating to many other systems
- Immediate response by Chief Information Security Officer (CISO).

2) Medium – departmental malware, phishing emails
- adversely impacts a moderate no. of systems/people
- individual department, building, unit
- non-critical enterprise system or service/departmental service
- moderate probability of propogation.

3) Low – spam emails, minor bugs/errors, minor n/w outages.
- small number of systems/people/n/w devices/segments
- little/no risk of propogation
- technical support staff must respond asap.

* Identify an incident – event mgmt, web interface, phone calls, emails.

Unit 4

Computer Forensics / Digital Forensics is a fusion of domains such
network forensics, server forensics, internet forensics, Social me
forensics, memory forensics, online gaming, data/disk forensics,
VR forensics.

Process : Digital Forensics

Identification - purpose, resources required

Preservation - isolate, secure, preserve data

Analysis - tools/techniques, process data

Documentation - of crime scene

Presentation - summarization & conclusion.

Locard's Principle of Exchange - whenever two objects come into contact with one another, an exchange of materials occurs b/
This may lead to a connection b/w a suspect & crime scene or suspect & victim based on transferred fragments of materials.

Digital Evidence is information and data of value to an investigati
that is stored on, received or transmitted by an electronic de

latent ?

crosses jurisdictional borders quickly

easily altered, damaged, destroyed

time sensitive.

Verify that an incident occurred
Restore business continuity
Determine how the attack was done
Improve security
Prosecute illegal activity

{ nessus
qualys
HAK5.org
Alpha cars }

→ Incident Response Team Responsibilities.

1) Preperation
2) Identification
3) Analysis
4) Containment
5) Mitigation
6) Reporting
7) Coordination
8) Training

→ Incident Response Team Roles.

1) Incident Response Manager
2) IT Security Analyst
3) Forensic Analyst
4) Network Security Engineer
5) Systems Administrator
6) Communications Coordinator
7) Legal counsel
8) Public Relations Specialist

→ Incident Management Process.

1) Preperation
2) Identification
3) Categorization
4) Prioritization
5) Investigation
6) Resolution
7) Reporting
8) Review & Improvement.

→ Goals of Incident Response.

1) Protecting systems from unauth access / damage / theft
2) Minimizing business disruption & financial impact
3) Ensuring compliance
4) Preventing negative reputation with customers
5) Cont. adapting to changing threat scenarios
6) Communication + Training + Support + Informed.

Why is incident prioritization important?

1) focus resources on high priority incidents
2) improve response time
3) align with business objectives
4) optimize resource allocation
5) ensure consistency.

Defn: Disaster Recovery Technologies are systems & tools that are designed to help organizations recover their critical IT systems & data after a disruptive event.

Examples: Data Backup & Recovery, Replication, Virtualization, cloud-based disaster recovery, high availability, disaster recovery testing

Impact of virtualization on Incident response & handling

Rapid provisioning, Isolation, Snapshots, Centralized Mgmt, Agility

Incident Reporting

1) Define Incident Reporting procedures
2) Train employees
3) Use a standardized incident reporting form
4) Ensure confidentiality
5) Evaluate Incidents
6) Learn from Incidents
7) Keep records.

Requirements of Incident Response Plan

A framework, skilled resource, latest tools, dedicated team, proper documentation, collaboration

→ Incident Reporting / Analysis / Response } 3 functions

Reporting: CERT, centralized mgmt, patterns of activity

Response: recovery, containment, prevention

SANS Institute Recommendations.

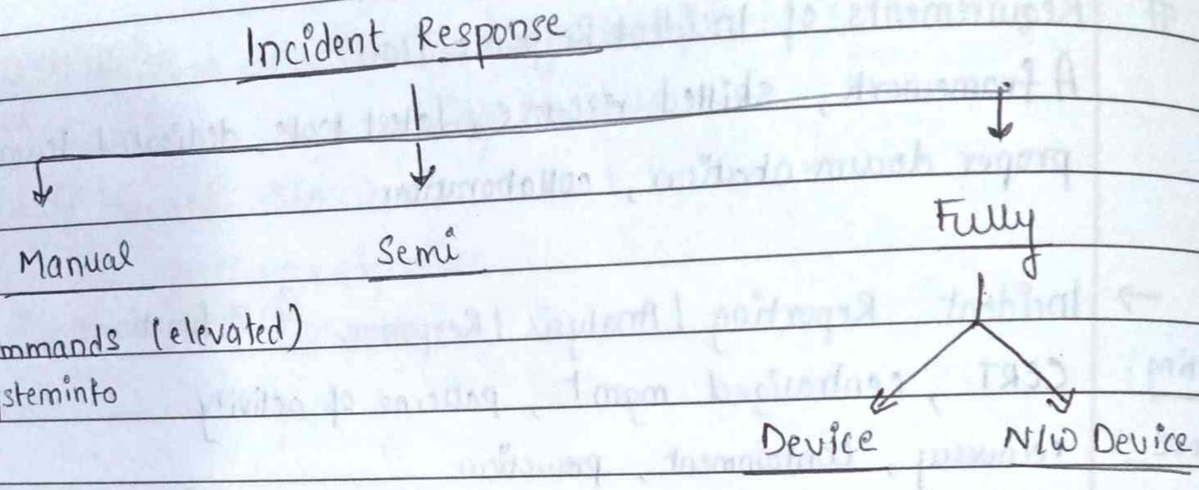
SysAdmin Audit Network & Security

- private US for profit company founded in 1989 (6 steps)

1) Preperation - risk ass., host security, n/w security, malware prevention, user awareness & training
2) Identification - Alerts (IDS/IPS, SIEM, AV), file integrity checking, TPM
   Public Info, People

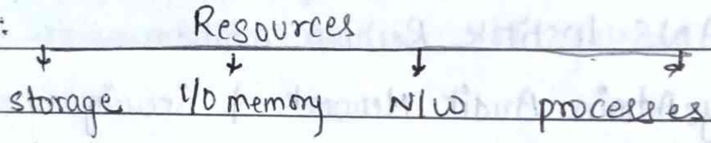
Attack Vectors: Ext/Removable media, web, email, impersonation

3) Containment
4) Eradication
5) Recovery
6) learning lesson



→ commands (elevated)

- systeminfo



* Context Switching :

switching resources b/w n resources.

Windows Artifacts Cheat Sheet

↓

objects that contain information about user activity on an operating system.

Process: Preperation → Identification → Containment → Eradication → Recovery → Lessons learned.

Memory: processes, opened files, registry keys & devices, n/w connections, encryption key & passwords, rootkits & memory only exploits, configuration settings.

Powercfg / SLEEPSTUDY

↓ Hibernation (>win 2000)

↓ DRIPS
Deepest Runtime Idle Platform State (triggers)

Mounting Method

↓ Block Device/ Readonly

↓ Block device/ writable

↓ FileSystem / Read Only

File Systems: FAT16 → FAT32 → EXFAT → NTFS → ReFS

FAT16
floppy disks

FAT32
32 bit, 4GB,
no security

EXFAT
USB & SD
cards

NTFS
64, 16TB
time stamp, Zone ID
~~volume shadow cpy~~

↓ Allocated & ↓ Unallocated

ReFS
Server

MFT: 1024 byte entries, 24 reserved entries, 12 system entries
$MFT, $MFTMirr, $LogFile, $Volume, :, $BitMap, $Boot,
$AttrDef, $BadClus, $Secure, $UpCase, $Extend

Zone ID:
-1: No Zone
0: My Comp.
1: Intranet
2: Trusted
3: Internet
4: Untrusted

Shadow Copy
(Volume Snapshot Service OR Volume Shadow Copy Service)

VSS Service
VSS Requester

→ restoring LUN, restoring files, data mining

SSD: Semiconductor based, non-volatile, proprietary, read/write is quick, wear levelling, trim.

Data Carving: extracting fragments (URL, chat sessions, email)

File carving: extracting files (word, pictures, archive)

IEF: Internet Evidence Finder.

Registry: system settings, application settings, device drivers, user profiles

NLA: Network Location Awareness.

CSC: 0, 16, 32, 48, 2048

TA1 - Notes

Reference: Chp - Computer Incident Response & Forensics.

Defn: An incident is an adverse event that is related to the safety and/or security of the information system.

Defn: Incident Response is the process of bringing together resources in an organized manner to deal with incidents.

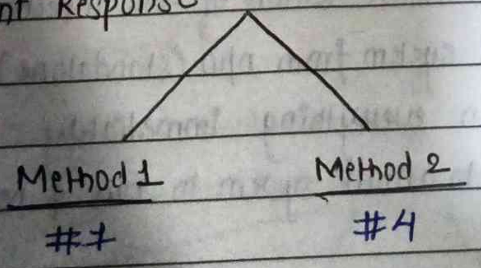
Objectives:

(a) Limit the immediate incident impact on business & customers
(b) Recover from the incident
(c) Determine how the incident occurred
(d) How to avoid further exploitation of the vulnerability
(e) Avoid escalation of further incident
(f) Assess the impact & damage
(g) Update corporate security policies & procedures.

Verify that an incident occ.
Improve security & IR
Prosecute illegal activity
Keep mgmt informed

SIRT: Security Incident Response Team; leader, members, legal counsel, staff; incident investigation; authority from highest levels of organization.

Stages of Incident Response



Each stage must be performed in sequence with the integrity of the system in mind.

Method 1

(1) Preperation -

- identification of the start of an incident & recovery
- establishment of corporate security policies
- training for incident responders (SIRT team)
- predeployed incident handling assets - sensors & probes, snapshots/ baselines & Configuration Management Database (CMDB), active auditing

(2) Identification -

- Is the event simply an unusual activity or can you classify it as malicious?
- Standardized Computer Incident Report.
- All investigative activities must be performed after a complete bit-stream copy is created on the system under investigation.

Level 1	Unauthorized Access	Level 4	Improper Usage
Level 2	Denial of Service	Level 5	Scans / Probes
Level 3	Malicious Code	Level 6	Investigation Incident

(3) Containment -

- Protect & keep available critical computing resources where possible
- Determine the operational status of the infected comp/sys/network.
  - (A) Disconnect system from n/w (standalone)
  - (B) Shut down everything immediately
  - (C) Continue to allow system to run & monitor activities.

vestigation – break off point for forensics
ermine the bredth & slope of incident
nponents & drives are considered as evidence.
ermine if involvement of law enforcement is required or not.

dication –
tting rid of the problem
anup – AV, deinstallations, rebuild, replace, reconstitute.
tification – to above & below the SIRT Manager.

overy –
urning the system/network/component to normal business operati
rvice restoration – implementation of contingency plans
stem/n/w validation – certifying the system as operational.

low Up – Lessons learned (post incident activity)
ective evaluation
gress is measured by making new mistakes, instead of the
me ones over & over again.

Method 2

eration → Detection & Analysis → Containment, Eradication, Reco
Post Incident Activity ←

ce: Slides - Incident Handling

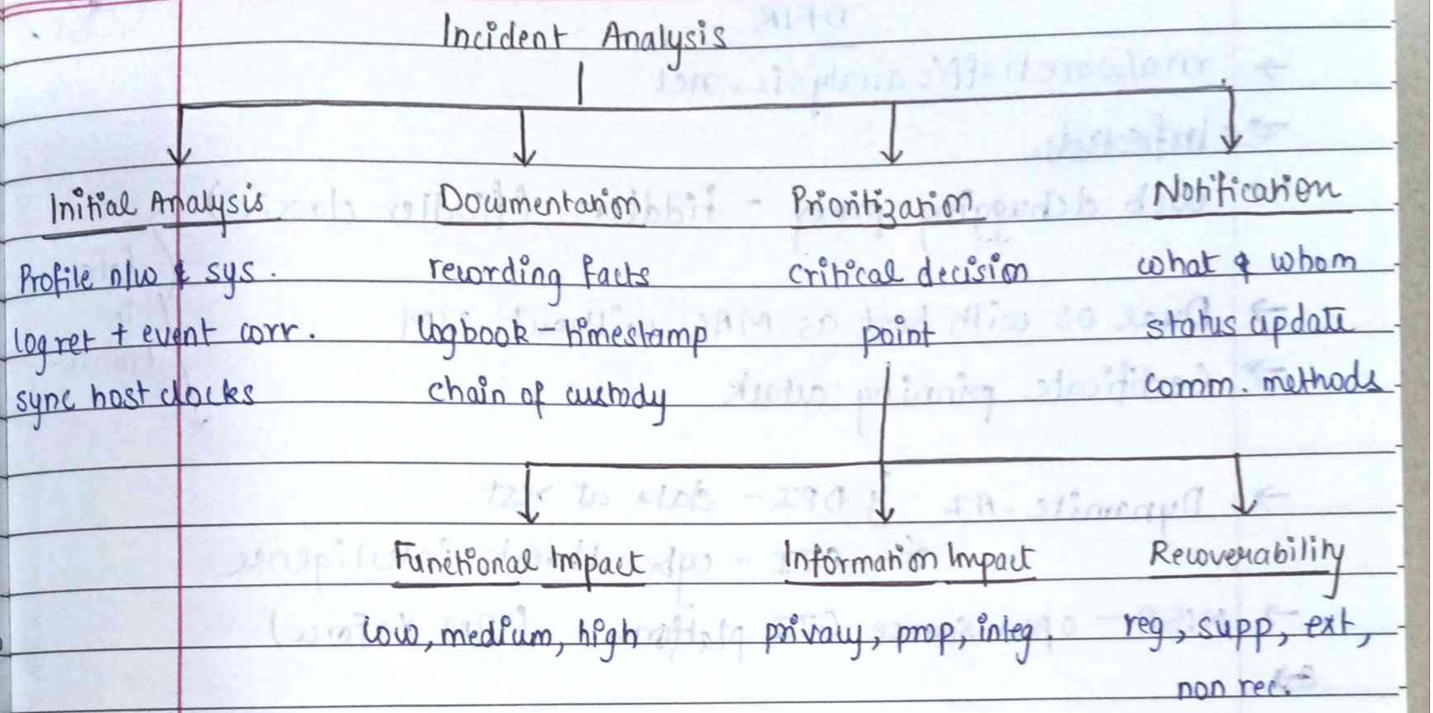
- Incident Response Plan - needed because attacks compromise
formal, foussed, coordinated approach to IR; roadmap; reso
& mgmt support required.

ments | | Requireme
on | Communication | Framework | Te
s | Metrics | Skilled Resource | Do
al | Roadmap | Tools | Co
ach | Relevance

Functions of Incident Handling

t Reporting | Incident Analysis | Incident
- central POC | Preventative strategy | Recovery, co
n in location | Incident report feedback | Network adr
information | Mitigation strategies | Share lesso
ine patterns | | CERT respon

SANS Institute - SysAdmin, Audit, Network Security; US
org; 1989; 6 step methodology



Incident Analysis

Initial Analysis
Profile n/w & sys.
log ret + event corr.
sync host clocks

Documentation
recording facts
logbook - timestamp
chain of custody

Prioritization
critical decision point

Notification
what & whom
status update
comm. methods

Functional Impact
low, medium, high

Information Impact
privacy, prop, integ.

Recoverability
reg, supp, ext, non rec.

DFIR

→ malwaretrafficanalysis.net

~~infectede~~

→ web debugging proxy - fiddler (fiddler classic) } data in transit

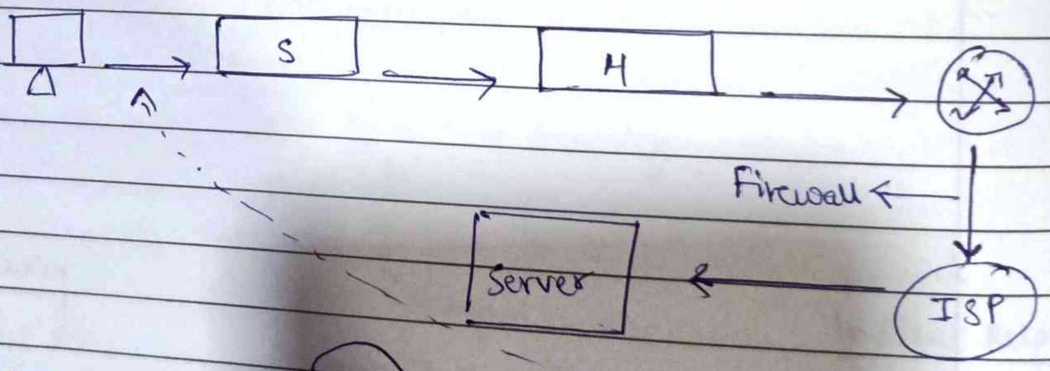
→ Dual OS with host as MAC without VM

→ Certificate pinning attack

→ Dynamite.AI } DPI - data at rest

← CTI - cyber threat intelligence

→ MISP - open source CTI platform (IBM X-Force)



→ Metadata & Payloads. SSL/TLS encrypted → certificate pinning

→ VX - underground (Nighthaide)