Section 10: Dealing with Incidents

118.Incident Response

**Entire Exam is pretty much based on the NIST 800-61 Computer Security Incident Handling Guide

Incident Response Process:
1. Preparation
1. The big Plan
2. Who is doing what
3. Organize the types of anticipated incidents

```
2. Reporting
        1. What reports go to whoms
        2. Escalation

3. Identification
        1. Recognize what incident has occured
        2. Reports from users
        3. check the monitoring tools you use
        4. Watch alerts and logs
        5. Assess the impact
        6. Define who is involved

4. Containment
        1. Mitigate the damage
        2. Stop the attack
        3. Segregate the network
        4. Shutdown the system
        5. turn off a service

5. Eradication
        1. Remove the malware
        2. Close off the vulnerability
        3. Add new controls

6. Recovery
        1. Restore from backups
        2. Pull from snapshots
        3. Hire replacement personnel
        4. Monitor to ensure good operations

7. Documentation
        1. Document the incident
        2. What failed
        3. what worked
        4. Generate a final report
```

Incident Response Plan

```
1. CIRT (Cyber incident Response Team)
        - A group of people whose job is to respond to all incidents
        - Full or part time - or both
        - IT security team
        - IT department
        - Human Resources
        - Legal
        - Public Relations

2. Document incident types/category definitions
        - Physical access
        - Malware
        - Phishing
        - Social Engineering
        - Data Access

3. Roles and Responsibilities
        - Users
        - Help desk
        - Human Resources
        - Database manager
        - Incident hotline
        - Incident Response manager/Incident Response Officer
        - Incident Response Team

4. Reporting Requirements/Escalation
        - Determine Severity
        - Based on severity have a clear chain of escalation
        - informing law enforcement

5. Practice
        - annual scenario drills
```

Quick Review

- Preparation is key to properly handling incidents
- Have a plan and execute it when incidents occur
- After any incident document everything

119.Digital Forensics

Takes place for one of two reasons:
1. Incident Occurs
2. Legal Hold

For the exam: Digital Forensics is basic

Chain of custody Process:
1. Define the evidence
2. Document the collection method
3. Date/Time Collected
4. Person(s) handling the evidence
5. Function of the person handling the evidence
6. All locations of the evidence

Order of Volitility (What do we get from the computer first?)
1. Memory
1. Caches
2. Routing Tables
3. ARP table

2. Data on the disc
    1. Optical media, flash drives
    2. Cache files, temp files
    3. Write blocker enabled tools

3. Remotely logged data
    1. Website data
    2. Remote file server logs

4. Backups
    1. Trends
    2. Low volitility but takes time to grab

Forensic Data Aquisition (checklist no order)

1. Capture the system image
2. Network traffic and logs
3. Capture Video
    1. Take video yourself of the workstation
    2. look for security cameras
    3. record time offset
    4. take audio/video off of the computer
4. Take hashes
5. Take Screenshots

```
6. Interview Witnesses
7. Track man hours
```

Quick Review:

- Forensics is the process of gathering data in such a way as to be presented in a court of law or some other formall inquiry
- The chain of custody maintains the integrity of the data/evidence gathered
- The order of volatility is a proces that enumerates when, where and how to gather the data/evidence before the data changes or disappears

---

120.Contingency Planning

1. Disaster Recovery (e.g. Hurricane):
    1. Back up sites:
        1. Cold site:
            - It takes week to bring online
            - Basic Office space: Buildings, chairs, AC
            - No operational equipment
            - Cheapest recovery site
        2. Warm Site:
            - Takes days to bring online
            - Operational equipment but little or no data
        3. Hot site
            - It takes hours to bring online
            - real-time synchronization
            - Almost all data ready to go - often just a quick update
            - Very expensive

        Things to Consider when thinking about backup sites:

        - Distance and location
        - Internet requirements
        - Housing and entertainment
        - Legal issues
2. Business Continuity (keeping things running):

    The order of restoration:

    Example:

```
1. Power
2. Wired LAN
3. ISP Link
4. Active Directory/DNS/DHCP servers
5. Accounting servers
6. Sales and accounting workstations
7. Video production servers
8. Video Production workstations
9. wireless
10. Periferals (Printers, cameras, scanners, faxes)
```

Annual Exercises:

```
- practice things e.g. moving servers to backup location
- Failover: The process of making back up sites happen
- Alternative processing sites
- Alternative business practices
- After action reporting
```

Review:

*Contingency planning attempts to mitigate adverse incidents to preserve business continuity

*Understand the pros and cons of the offsite options available: cold site, ware site, hot site

*Thorough planning and practice is what makes recovery plans successful when disasters occur

121.Backups

Backup methods

```
1. Backup of everything = full backup

        File systems
                - Have features that help know when a file has been changed

                cmd stat file - linux
                archive attribute - windows

2. Differential Backup - Backup of all the changes since the last full
backup (less back up sets but bigger)
3.Incremental Backup - Only backs up changes made from last back up (More
back up sets but smaller)

4. Snapshots - typically on virtual machines

5. Local Back ups - e.g. tapes, external hard drives (Conviently close,
```

easy)
Offsite back ups- (Not as convient, but safer from local fires etc)

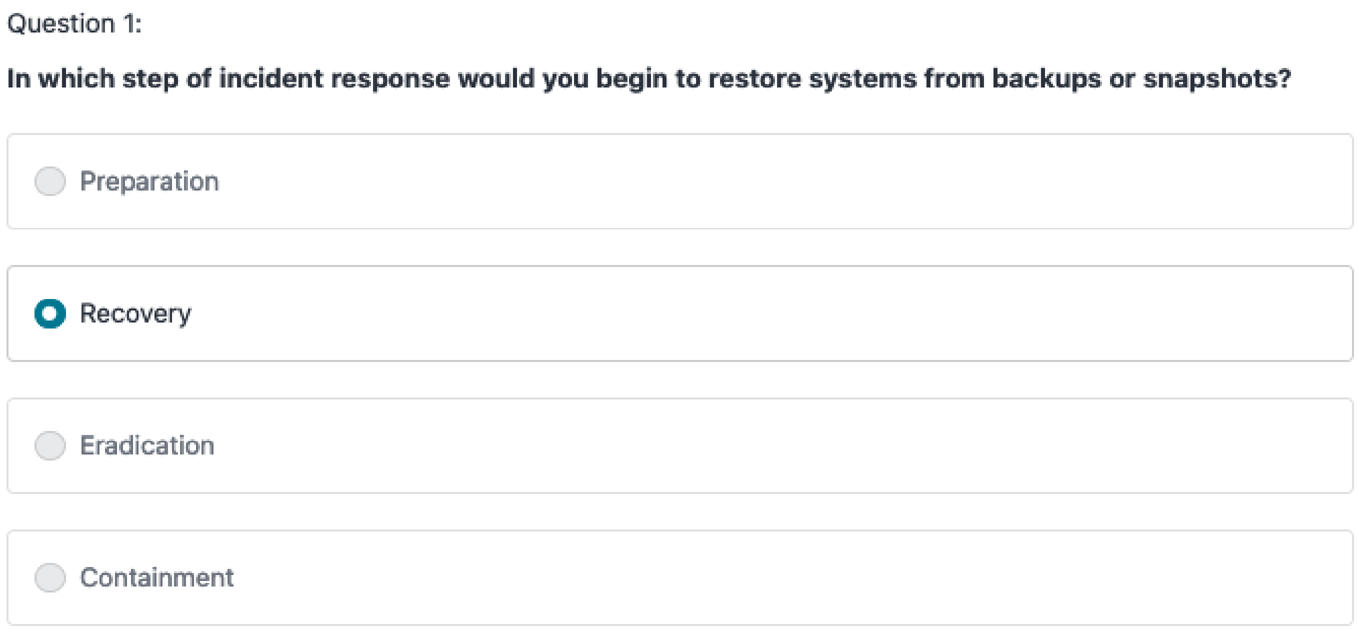
6. Local Backups + Offsite backups are best.

7. Cloud backups - They take up a lot of time to get the initial backups going, however there is continuous ongoing incrememtal backups once they are set up.

Quick Review:

*Understand the differences between an incremental and differential backup
*Snapshots are typically used with virtual machines and are usually not stored on separate media
*Be able to describe the pros and cons of local vs. remote vs. cloud-based backups

Quiz



Question 1:

In which step of incident response would you begin to restore systems from backups or snapshots?

○ Preparation

● Recovery

○ Eradication

○ Containment

Question 2:

Which of the following does NOT fall under chain-of-custody?

○ Documenting all locations of evidence

● Write block

○ List of all person(s) handling evidence

○ Defining what constitutes evidence

Question 3:

Which type of recovery site has no equipment or data and is just a basic office space?

○ Hot site

○ Warm site

● Cold site

○ Offsite

Question 4:

Which of these backup types only backs up data that has changed since the last full backup?

○ Incremental backup

○ Snapshot

○ Full backup

● Differential backup