VARE Lecture 8 & 9

Here are **concise exam prep notes** covering all major content from **VARE Lecture 8** and **VARE Lecture 9**:

VARE Lecture 8: ITS Vulnerability Management Procedure

Purpose & Scope

- Prevent, detect, and mitigate technical vulnerabilities.
- Ensure confidentiality, integrity, and availability of sensitive data.
- Applies to all staff, contractors, and third parties.

Key Roles & Responsibilities

- **CISO**
  - Develop standards, choose tools, review program quarterly.
  - Review results, determine mitigation strategy.
- **ITS**
  - Implement tools, keep scanners updated.
  - Ensure only trained personnel perform assessments.
- **Sys/App Admins**
  - Monitor, schedule, report, and respond to vulnerabilities.
- **Sys/App Owners**
  - Coordinate tests with minimal disruption, ensure remediation.
- **Management**
  - Provide resources and review results.
- **Third Parties**
  - Must maintain their own vulnerability programs.

Types of Assessments

1. **Perimeter Vulnerability Assessment (PVA)**
    - External perspective; scan ports, services, protocols.
2. **Internal Vulnerability Scan (IVS)**
    - Detect missing patches, weak passwords, misconfigs.
3. **Network Security Assessment (NSA)**
    - Audit controls, access policies, change logs, etc.
4. **Web Application Assessment**
    - Identify and verify vulnerabilities via scanning and analysis.
5. **Wireless Security Assessment (WSA)**
    - Detect rogue APs, misconfigurations, missing patches.
6. **Security Test & Evaluation (ST&E)**
    - Pre-production testing of new systems.
7. **Application Security Assessment**
    - Review input validation, access controls, config, logging.
8. **Unauthorized Device Scan**
    - Weekly scan to detect unknown hardware/software.
9. **Preventative Malware Assessment**
    - Evaluate protection on systems not normally scanned.

Mitigation & Documentation

- Vulnerabilities must be analyzed, prioritized, and remediated.
- Assessment reports must be kept for **6 years**.
- Exceptions handled via formal policy.

Assessment Schedule

Assessment Type	Frequency
PVA	Annually
IVS, NSA, Web, App Security	Quarterly

Assessment Type	Frequency
WSA	Annually
Unauthorized Devices	Weekly
ST&E	Pre-production

VARE Lecture 9: Best Practices for Vulnerability Assessment & Management (VAM)

Why VAM Is Crucial

- Other tools (firewall, AV, IPS) only partially protect.
- VAM identifies **known weaknesses** before attackers do.
- Attacks mostly use **known vulnerabilities**, not zero-days.

7 Best Practices

1. **Budget properly:**
   ⅓ for tools, ⅔ for fixing vulnerabilities.
2. **Scan broadly:**
   Cover everything; prioritize perimeter.
3. **Scan accurately:**
   Minimize false positives/negatives.
4. **Scan frequently:**
   Weekly/daily scans recommended.
5. **Track changes over time:**
   Know if your network is getting better or worse.
6. **Use credentialed scans for high-value targets.**
7. **Fix high-risk vulnerabilities.**

Accuracy in VAM

- **False Positives:** Waste time.
- **False Negatives:** Leave you exposed.
- **Behavioral Testing > Version-based Testing**
    - Tests real responses instead of relying on software versions.

Network Security Strategy

- **Fixing vulnerabilities is more effective than just adding firewalls.**
- A well-patched, hardened host is better than high, fragile perimeter defenses.

Patching Challenges

- Too many patches = overwhelmed staff.
- Not all vulnerabilities need patching—some are mitigated by config.
- VAM helps identify **which patches matter**.

VAM for Large/Complex Networks

- Free tools aren’t enough for:
    - Large, distributed networks.
    - Compliance-heavy environments (e.g., PCI-DSS, HIPAA).
- VAM tools must be scalable and provide reliable reports.

Modern Challenges

- Many networks ignore or delay patching due to:
    - Limited budget/resources.
    - Organizational culture focused on perimeter defense.
- VAM often seen as a checkbox, not an active defense layer.

Takeaway

- **VAM is now essential**: Accurate, broad, frequent scanning and prioritization.
- **Fix vulnerabilities first**, then build walls.
- Good VAM solutions support **automated, prioritized, and behavior-based** scanning.

Let me know if you want **flashcards, diagrams, or quiz questions** to help you revise faster.