Below is a comprehensive, sentence-by-sentence breakdown of the document **“Removing Malware Notes.docx”** converted into professional **study notes**, structured and formatted specifically for **CompTIA A+ 220-1102 (Objective 2.4 – Security)**. It’s fully optimized for direct pasting into **Microsoft Word** — with numbered topics, clean bullet points, minimal spacing, and no reformatting needed.

**🧹 Removing Malware – Study Notes - CompTIA A+ 220-1102 | Objective 2.4 – Security**

**1. Confirm Symptoms and Identify Malware**

* If a system displays signs of infection (e.g., slow performance, strange files, or gibberish text), the first step is to **scan the computer** to verify the presence of malware.
* Run a reputable **antivirus or anti-malware scan** to confirm whether the system is infected.

**2. Backup Before Cleanup**

* **Before removing malware**, always perform a **full backup** of the current system.
* This is important because:
  + Filesystems or configurations may need to be altered.
  + In some cases, a **complete reinstall** might be necessary.
  + Backups ensure that personal data is not lost during cleanup.

**3. Identify the Symptoms**

* Observe what the computer is doing that indicates infection:
  + New/unexpected files
  + Unusual slowness
  + Gibberish on-screen
* Documenting symptoms can help determine **which type of malware is present**.

**4. Quarantine the Affected System**

* Quarantine involves **isolating the infected machine** to stop the malware from spreading.
* Do this by:
  + **Unplugging the network cable** or
  + **Disabling the network interface card (NIC)**
* This prevents further communication with other systems.

**5. Disable System Restore (Windows Only)**

* **System Restore should be disabled** to prevent malware from being stored in restore points.
* Malware may persist if a user reverts to a restore point that was created during the infection.
* Steps:
  + Turn off System Restore
  + Delete all previous restore points to avoid reinfection

**6. Remediate the System**

* Remediation involves **actively removing malware** using antivirus tools.
* Key actions include:
  + **Updating antivirus/anti-malware definitions**
  + Rebooting into **Safe Mode** to reduce file locks
  + Running a scan in a **Pre-installation Environment (PE)** for deep system cleaning
* Safe Mode helps by ensuring that **fewer system files are active**, increasing the chances of malware removal.

**7. Schedule Updates and Scans**

* After cleanup, **enable automatic updates** and configure **regular antivirus scans**.
* This prevents reinfection by ensuring virus definitions are always current.
* Recommended scan frequency: **at least weekly**.

**8. Re-enable System Restore**

* Once malware is removed, turn **System Restore back on**.
* Immediately create a **new restore point**, labeled as a **“known good backup”**.
* This provides a fallback option in case future issues arise.

**9. User Security Awareness Training**

* A major source of malware infections is **user error** (e.g., clicking malicious links).
* Provide **training on safe computing practices** to prevent repeat infections.
* Effective training includes:
  + Recognizing phishing attempts
  + Avoiding suspicious downloads
  + Using strong passwords
  + Understanding email attachment risks

**10. Boot Sector Virus Removal**

* Boot sector viruses require scanning from **an external bootable device** (USB, CD/DVD).
* This avoids triggering the virus, which loads from the boot sector during normal startup.
* By booting externally, antivirus software can scan and clean the internal drive safely.

**11. Alternative Removal Method: External Scanning**

* Another method is to **physically remove the infected drive** and connect it to a **clean system** as a **secondary drive**.
* The clean host scans the infected drive without executing its system files.
* This method avoids active malware interference and often results in more effective cleaning.