Post-Attack Remediation Steps for Windows Systems

Steps for remediation:

1. Audit Accounts

- Check for new additions, remove any unrecognized or stale accounts. Ensure that only authorized users have administrative privileges.

2. Check for Persistence Mechanisms

- Use tools like Autoruns from Sysinternals to review startup items, scheduled tasks, and WMI objects for anything suspicious.

  https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

3. File System and OS Integrity

- Inspect **\Device\HarddiskVolume*\Windows\System32** for any suspicious files and delete them.
- Run sfc /scannow to check and repair the integrity of OS files.

4. Reset AD User Accounts

- Reset passwords for all AD users.
- Reset the Krbtgt account twice following the steps outlined in Microsoft's guide.

  https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password

5. Firewall and Remote Access

- Ensure no rules allow RDP (3389 by default) or other remote access ports to be exposed to the internet.
- Check for non-standard remote access ports and ensure they are disabled from being internet-facing if possible.

6. Network and DNS Configuration (Based upon attack priority)

- Change the system's name and IP address to disrupt the attacker's connections.
- Update DNS names to point to new IP addresses, reducing the risk of further compromise.

7. Use Sysinternals Suite for In-depth Analysis

- Process Explorer: Provides detailed information on running processes.
- Process Monitor: Shows real-time file system, registry, network, and process activity.
- TCPView: Maps listening TCP and UDP ports back to the owning process.

https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

Post-Attack Remediation Steps for Linux Systems

1. User Account Auditing

- Focus on accounts with elevated privileges (e.g., root or sudoers). Remove any unnecessary or unrecognized accounts.
- Command: **cat /etc/passwd**, **cat /etc/group, cat /etc/sudoers**

2. Startup Processes, Services, and Scheduled Jobs, Cron Jobs

- Review system services using **systemctl** commands.
- Review traditional init scripts in **/etc/init.d/** and **/etc/rc*.d/** directories.
- Command: **systemctl list-unit-files --type=service, chkconfig --list, ls /etc/rc*.d/**
- Check for unauthorized or suspicious cron jobs.
- Command: crontab -l, ls /etc/cron.*

3. Critical System Directories

- **Review Critical System Directories:**
    - Check **/bin**, **/sbin**, **/usr/bin**, **/usr/sbin**, **/etc** for suspicious or unexpected files or binaries.
    - Use tools like **rpm -V** or **debsums** to verify the integrity of installed packages against the package manager's database.
    - Command: **rpm -Va**, **debsums -c**

4. Firewall Rules and Network Configuration

- **Audit Firewall Rules:**
    - Ensure only necessary ports and services are exposed.
    - Command: **iptables -L**, **firewall-cmd --list-all**
- **Review External Access Rules:**
    - Disable any unnecessary services or ports facing the internet.
    - Command: **netstat -tuln**, **ss -tuln**, **lsof -i**

5. Network Connections and Processes

- **Check for Open Network Connections:**
    - Use **netstat**, **ss**, or **lsof** commands to check for open network connections and associated processes.
    - Command: **netstat -tulnp**, **ss -tulnp**, **lsof -i**

6. Sudo Access and Logs

- **Ensure Proper Configuration of Sudo Access:**
    - Monitor sudo logs for suspicious activities.
    - Command: **visudo**, **cat /var/log/auth.log | grep sudo**

7. File Integrity Monitoring

- **Utilize File Integrity Monitoring Tools:**
    - Use tools like AIDE (Advanced Intrusion Detection Environment) for monitoring file integrity.
    - Command: **aide --check**

8. System Updates and Patches

- **Ensure System is Up-to-date:**
    - Regularly install the latest security patches and updates using package managers (**apt**, **yum**, **dnf**, etc.).
    - Command: **apt update && apt upgrade -y**, **yum update -y**, **dnf update -y**

9. System Logs

- **Configure and Monitor System Logs:**
    - Set up and configure system logs using **syslog** or **journalctl** to monitor for suspicious activities.
    - Command: **journalctl -xe**, **cat /var/log/syslog**, **cat /var/log/messages**

10. Backup Strategy

- **Implement a Robust Backup Strategy:**
    - Ensure critical system files and data are regularly backed up and can be restored if needed.
    - Tools: **rsync**, **tar**, **backup software**

11. Security Scans and Audits

- **Perform Comprehensive Security Scans:**

- Use tools like Lynis, OpenVAS, or Nessus for detailed security scans and audits of the system.
- Command: **lynis audit system**, **openvas-start**, **nessuscli scan list**

12. Additional Steps for Enhanced Security (*Based upon attack priority)*

- **Move System to a New Name/IP Address:**
  - Change the system's hostname and IP address to disrupt the attacker's access.
  - Command: **hostnamectl set-hostname newhostname, ip addr add new_ip_address dev eth0**
- **Null Routing Particular IP Addresses:**
  - Null route any known malicious IP addresses.
  - Command: **ip route add blackholed_ip dev null0**
- **Changing DNS Names:**
  - Update DNS names to point to new IP addresses.
  - Command: Update DNS records with your DNS provider.

Post-Attack Remediation Steps for MacOS Systems

1. User Account Auditing

- **Review All User Accounts:**
  - Focus on accounts with elevated privileges (e.g., root, admin).
  - Remove any unnecessary or unrecognized accounts.
  - Command: **dscl . list /Users, dscacheutil -q group**

2. Startup Processes, Services, and Scheduled Jobs

- **Check Startup Processes and Services:**
  - Ensure only necessary and authorized programs are configured to start automatically.
  - Review system services using **launchctl** commands and **LaunchDaemons/LaunchAgents in /Library/LaunchDaemons, /Library/LaunchAgents, and /System/Library/LaunchDaemons.**

    - Command: **launchctl list, ls /Library/LaunchDaemons, ls /Library/LaunchAgents**
- **Review Cron Jobs:**
    - Check for unauthorized or suspicious cron jobs.
    - Command: **crontab -l, ls /etc/cron.***

3. Critical System Directories

- **Review Critical System Directories:**
    - Check /**bin, /sbin, /usr/bin, /usr/sbin, /etc** for suspicious or unexpected files or binaries.
    - Use **pkgutil** to verify the integrity of installed packages.
    - Command**: ls -l /bin /sbin /usr/bin /usr/sbin /etc, pkgutil --check-signature**

4. Firewall Rules and Network Configuration

- **Audit Firewall Rules:**
    - Ensure only necessary ports and services are exposed.
    - Use the built-in macOS application firewall and **pf (Packet Filter).**
    - Command: **sudo /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate, sudo pfctl -sr**
- **Review External Access Rules:**
    - Disable any unnecessary services or ports facing the internet.
    - Command: **netstat -an, lsof -i**

5. Network Connections and Processes

- **Check for Open Network Connections:**
    - Use **netstat, lsof, or Activity Monitor** to check for open network connections and associated processes.
    - Command: **netstat -tuln, lsof -i, sudo lsof -PiTCP -sTCP:LISTEN**

6. Sudo Access and Logs

- **Ensure Proper Configuration of Sudo Access:**
    - Monitor sudo logs for suspicious activities.
    - Command: **sudo cat /var/log/system.log | grep sudo**

7. File Integrity Monitoring

- **Utilize File Integrity Monitoring Tools:**
    - Use tools like **fs_usage or fseventer** for monitoring file integrity.
    - Command: **sudo fs_usage**

8. System Updates and Patches

- **Ensure System is Up-to-date:**
    - Regularly install the latest security patches and updates using softwareupdate.
    - Command: **softwareupdate -l, softwareupdate -i -a**

9. System Logs

- **Configure and Monitor System Logs:**
    - Set up and configure system logs using syslog or log to monitor for suspicious activities.
    - Command: **log show --predicate 'eventMessage contains "sudo"' --info, cat /var/log/system.log**

10. Backup Strategy

- **Implement a Robust Backup Strategy:**
    - Ensure critical system files and data are regularly backed up and can be restored if needed.
    - Use **Time Machine** for backups.
    - Command: **tmutil startbackup**

11. Security Scans and Audits

- **Perform Comprehensive Security Scans:**
    - Use tools like KnockKnock, BlockBlock, or Malwarebytes for detailed security scans and audits of the system.

12. Additional Steps for Enhanced Security (*Based upon attack priority)*

- **Move System to a New Name/IP Address:**
    - Change the system's hostname and IP address to disrupt the attacker's access.
    - Command: **sudo scutil --set HostName newhostname, sudo ipconfig set en0 new_ip_address**
- **Null Routing Particular IP Addresses:**
    - Null route any known malicious IP addresses.

- Command: **sudo route add blackholed_ip -interface lo0**

- **Changing DNS Names:**
  - Update DNS names to point to new IP addresses.
  - Command: Update DNS records with your DNS provider.

13. Additional Tools and Techniques

- **Sysinternal Suite of Tools:**
  - Activity Monitor: For process and resource monitoring.
  - Console: For log monitoring.
  - Little Snitch: For network monitoring and control.

  https://support.apple.com/en-in/guide/activity-monitor/welcome/mac
  https://support.apple.com/en-in/guide/console/welcome/mac
  https://www.obdev.at/products/littlesnitch/index.html
- **Check for Hidden Processes and Files:**
  - Use tools like **KnockKnock and BlockBlock** to check for hidden processes and files.
  - **Command:** Download and use from Objective-See

    https://objective-see.org/
- **Verify Kernel Extensions:**
  - Check for unauthorized or suspicious kernel extensions.
  - Command: **kextstat, kextunload <extension>**

Best Practices: -

-- Promote use of strong, unique passwords and MFA to protect accounts
-- Emphasize the importance of keeping system and software up to date to address vulnerabilities
-- Prioritize ongoing security awareness training to educate employees about recognizing and responding to threats like phishing.
-- Limit data access to authorized individuals and classify sensitive data for appropriate security measures.
-- Stress the need of monitoring and periodic internal and external security audits to detect and address weakness.
-- Regular data backups for effective mitigations and recovery in the event of security breach.