**RISK ASSESSMENT REPORT: RESPONDING AND RECOVERING A HACKED COMPUTER**

**1. Introduction** This report outlines the methods used to respond and recover a compromised computer system. It includes risk assessment, response strategies, and recovery measures to restore system integrity and prevent future attacks.

**2. Risk Assessment**

**Incident Overview:**

* Date of Incident: March 20, 2025
* Affected System: Windows Server 2019
* Nature of Attack: Unauthorized access and malware infection
* Impact: Data breach, system slowdown, potential data loss

**Threat Analysis:**

* **Attack Vector:** Phishing email leading to malware installation
* **Severity:** High (Confidential files compromised)
* **Vulnerabilities Exploited:** Outdated software, weak credentials

**3. Response Methods**

**Step 1: Containment**

* **Isolate the System:** Disconnect the compromised computer from the network to prevent further spread.
* netsh interface set interface "Wi-Fi" admin=disable
* netsh interface set interface "Ethernet" admin=disable
* **Disable Unauthorized Access:** Lock compromised accounts and change all credentials.
* net user [username] /active:no
* net user [username] [NewPassword]
* **Identify Malicious Processes:** Use Task Manager and PowerShell commands to detect suspicious processes.
* tasklist | findstr /i "suspicious\_process"
* Get-Process | Where-Object { $\_.ProcessName -like "\*malware\*" }

**Step 2: Eradication**

* **Remove Malware:** Run antivirus and anti-malware scans using Windows Defender.
* MpCmdRun.exe -Scan -ScanType 2
* **Delete Malicious Files:** Locate and remove unauthorized executables in system directories.
* del /F /Q C:\Users\Public\malware.exe
* **Patch Security Gaps:** Apply the latest security updates and install a firewall.
* wuauclt /detectnow /updatenow
* netsh advfirewall set allprofiles state on

**Step 3: Incident Investigation**

* **Review Logs:** Use Event Viewer to check login attempts and system modifications.
* wevtutil qe Security /c:10 /rd:true /f:text
* **Trace Attack Origin:** Analyze firewall logs to identify the source of the attack.
* netsh firewall show state

**4. Recovery Methods**

**Step 1: System Restoration**

* **Restore from Backup:** If available, restore the system from a clean backup created before the attack.
* wbadmin start recovery -version:[backup-version]
* **Reinstall OS if Needed:** If the infection is severe, perform a clean reinstall of the operating system.
* bootrec /fixmbr
* bootrec /fixboot
* bootrec /scanos
* bootrec /rebuildbcd

**Step 2: Strengthening Security**

* **Implement Multi-Factor Authentication (MFA):** Require two-factor authentication for critical accounts.
* **Use Strong Passwords:** Enforce password policies to require complex passwords.
* net accounts /minpwlen:12 /maxpwage:30
* **Limit User Privileges:** Assign minimal permissions necessary for users.
* icacls "C:\SensitiveData" /grant User:(R)

**Step 3: Monitoring and Future Prevention**

* **Deploy Intrusion Detection System (IDS):** Implement an IDS to detect unusual network activities.
* **Conduct Security Training:** Educate employees on phishing and cybersecurity best practices.
* **Perform Regular Audits:** Schedule periodic security audits to detect vulnerabilities early.
* Get-WinEvent -LogName Security | Format-Table -AutoSize

**5. Conclusion** Responding to and recovering from a cyberattack requires swift action, thorough investigation, and proactive security measures. By following structured response steps and strengthening security protocols, organizations can minimize damage and prevent future incidents.