RWANDA POLYTECHNIC

MUSANZE COLLEGE

DEPARTMENT: ICT

PROGRAM: INFORMATION TECHNOLOGY

RQF LEVEL: 8

MODULE: CYBERSECURITY

Academic: 2024-2025

ASSISSGNMENT 4

Date: 2/04/2025

Name: NIYIGABA Claude

Reg No: 24RP14647

Responding to and Recovering from a Hacked Computer

When a computer is hacked, it's crucial to respond quickly and methodically to minimize damage and restore security. The process involves five key steps:

1. Identification (Detection)

The first step is to identify the breach as soon as possible. Signs of a hack include:

- Slow system performance, crashes, or unexpected restarts.
- Unusual network activity, such as unfamiliar logins or high data usage.
- Ransomware messages, pop-ups, or unauthorized file changes.

1. Detection Tools & Techniques:

- Intrusion Detection Systems (IDS): Monitors and alerts on suspicious activity.
- Security Information and Event Management (SIEM): Analyzes security logs for threats.
- Antivirus & Anti-malware Software: Scans for and removes malicious files.
- Regular System Audits: Helps detect unauthorized changes or vulnerabilities.

2. Containment

Once a hack is confirmed, the next step is to contain the damage.

2. Immediate Actions:

- Disconnect the affected system from the network to prevent further spread.
- Preserve logs and timestamps for forensic analysis.
- Change passwords and access controls for compromised accounts.

3. Containment Strategies:

- Short-term containment: Focuses on stopping immediate threats.
- Long-term containment: Strengthens security to prevent re-entry.

3. Eradication

After containment, remove all traces of the attack from the system.

4. Steps to Remove the Threat:

- Delete malware, rootkits, and malicious files.
- Patch security vulnerabilities exploited in the attack.
- Update security configurations to prevent similar breaches.
- Enhance endpoint security to protect devices from future attacks.

Since hackers often leave hidden access points, this step requires thorough technical analysis to ensure complete removal.

4. Recovery

After eradicating the threat, restore the system to normal operations.

5. Key Recovery Steps:

- Restore data from secure backups (ensure backups are clean).
- Test the repaired system to verify security and functionality.
- Monitor for unusual activity to detect any lingering threats.
- Document the incident for future reference and improvement.

5. Prevention

The final step is to strengthen security to prevent future attacks.

6. Best Practices for Prevention:

- Implement stronger security measures (encryption, multi-factor authentication).
- Regularly update and patch all systems and software.

- Train employees to recognize phishing and other cyber threats.
- Continuously monitor security to detect vulnerabilities early.

7. Recommended Security Tools:

- Endpoint Detection & Response (EDR): Detects advanced threats.
- Regular Vulnerability Scanning & Penetration Testing: Identifies weaknesses.
- Security Frameworks (ISO 27001, NIST, CIS Controls): Ensures best practices.

By following these five steps, organizations can effectively respond to cyberattacks, recover safely, and build stronger defenses against future threats.