**Incident Response Report: Ransomware Attack Simulation**

**1. Initial Detection**

IT Security receives an alert from the antivirus system and SIEM (Security Information and Event Management) indicating abnormal encryption activity on a file server. The affected system is identified through:

* Unusual CPU and disk activity logs.
* A spike in outbound traffic to suspicious IP addresses.
* File extensions being renamed (e.g., .encrypted).

**Documentation Includes:**

* Timestamp of alert.
* Hostname/IP address of affected server.
* User account involved.
* Malware signature and hash (if available).
* Screenshots of the ransomware message (if present).

**2. Incident Identification**

**System Logs and IoC Analysis:**

* Review Windows Event Logs (IDs 4624, 4672, 4688 for suspicious logins and process executions).
* Examine Sysmon logs for process creation and network connections.
* Collect IoCs (file hashes, domain names, IPs, email subject, sender).

**Network Traffic:**

* Analyze packet captures using **Wireshark** or **Zeek**.
* Look for C2 traffic patterns or data exfiltration attempts.

**Tools Used:**

* Windows Event Viewer
* Zeek (for PCAP analysis)
* RITA (to detect beaconing)
* YARA rules for malware matching

**IoC Search:**

* Run scripts with PowerShell or Sysinternals tools to scan endpoints.
* Use EDR tools to search and isolate compromised assets.

**Scope Determination:**

* Cross-reference affected user logins with AD logs.
* Identify lateral movement via remote desktop or SMB.

**Compromise Identification:**

* Email headers show spoofed internal domain with malicious attachment.
* User “jdoe” opened the attachment, triggering the infection.

**3. Containment**

**Measures:**

* Isolate infected server and workstations.
* Disable affected user accounts.
* Block known malicious IPs/domains in the firewall.
* Temporarily disable file sharing services (SMB).

**Communication to Users:**

Subject: Immediate Security Alert – Action Required

We have identified a security incident involving ransomware. Please DO NOT open any suspicious emails or attachments. If your system behaves unusually or files become inaccessible, report it immediately. IT is working to contain the threat and will keep you informed. Thank you for your cooperation.

**4. Eradication**

**Isolation:**

* Use VLAN segmentation or physically disconnect infected systems.
* Clone affected systems for forensic analysis.

**Malware Removal:**

* Use tools like Windows Defender Offline, Malwarebytes, or ESET.
* Remove registry changes, scheduled tasks, and persistent services.

**5. Recovery**

**Plan:**

* Restore systems from last clean backup (prior to infection).
* Prioritize:
  1. Domain Controllers
  2. File Servers
  3. Email Servers
  4. Web Servers
  5. User Workstations

**Time Estimate:**

* 24–72 hours, depending on system criticality and backup speed.

**Communication to Stakeholders:**

* Daily status updates.
* Recovery milestones.
* Timeframes for each system class.

**6. Post-Incident Analysis**

**Lessons Learned:**

* Users need phishing awareness training.
* Email filters and antivirus missed zero-day ransomware.

**Improvements:**

* Deploy endpoint detection & response (EDR).
* Implement better email filtering (sandboxing attachments).
* Enforce least privilege on user accounts.

**Documentation:**

* Full timeline of the incident.
* Summary of compromised assets.
* Root cause analysis.
* Steps taken and response times.

**7. Conclusion**

The ransomware incident demonstrated the importance of fast detection, cross-functional communication, and robust backups. Investing in training, updated security tools, and an improved incident response playbook will better prepare us for future threats.

**Recommended Resources:**

* NIST SP 800-61r2 (Computer Security Incident Handling Guide)
* SANS Incident Handler’s Handbook
* MITRE ATT&CK framework

**Assessment Answers:**

1. **C.** Minimizing the impact of a security breach
2. **C.** Eradication
3. **C.** To guide the organization’s response to security incidents
4. **B.** Many attacks are not detected in real-time
5. **C.** Computer Security Incident Response Team
6. **C.** OpenIOC
7. **A.** Isolation
8. **C.** Restoring systems from backups
9. **C.** To adapt to evolving threats and improve response capabilities
10. **B.** Preserving evidence for potential legal action