### ***Penetration Testing Engagement Report for Healthcare Infrastructure***

### **1. Description of the Scope and Penetration Testing Method**

**Services Provided:** The penetration test conducted for this hospital included an assessment of both internal and external network infrastructure security, as well as employee behavior in response to social engineering attacks. The activities were divided into the following components:

* **Technical network-level penetration testing – internal network:** Identification and exploitation of network vulnerabilities within the hospital's internal networks.
* **Technical network-level penetration testing – external network:** Evaluation of the security of hosts exposed to the internet and the potential for an external attack.
* **Social engineering – phone-based phishing:** Testing employee responses to phishing phone calls.
* **Social engineering – email phishing:** Simulating phishing email attacks to evaluate employee behavior.

**Testing Methods Used:**

1. **Reconnaissance and Scanning:** Scanning ports and services to identify vulnerable entry points.
2. **Exploitation:** Leveraging identified vulnerabilities, including SMB EternalBlue exploits, to gain root-level access on systems.
3. **Social Engineering:** Sending phishing emails and conducting phone calls to manipulate employees and obtain access or sensitive information.

### **2. Brief Description of the Testing Scope**

**Tested Areas:**

* **Internal Network:** All devices and servers connected to the hospital’s internal network were included in the testing.
* **External Network:** Testing was conducted on devices and servers accessible via the internet (e.g., web servers, email servers, etc.).
* **Employees:** Social engineering attacks were simulated to evaluate how employees react to phishing and phone-based manipulation attempts.

**Internal Network Testing Results:**

1. **Vulnerability Scanning:**
   * The scans revealed multiple security vulnerabilities in the internal networks.
   * Open ports and insecure versions of critical services were identified.
2. **Exploitation of Vulnerabilities:**
   * The SMB EternalBlue vulnerability (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) was used to compromise several critical systems, including McAfee security servers.
   * After compromising the McAfee server, the attacker obtained root access to the affected systems.
3. **Access to Sensitive Files:**
   * Once root access was achieved, sensitive files were identified and accessed, including patient information and payment details.

### **3. Actions Taken**

**Performed Actions:**

1. **Internal Network Testing:**
   * **Port and Service Scanning:** Scans were performed to identify open ports and vulnerable services.
   * **Vulnerability Exploitation:** EternalBlue was exploited to access servers and gain root privileges.
2. **Social Engineering – Phone Phishing:**
   * Simulated phishing phone calls were made to evaluate employee responses and attempt to obtain access information.
3. **Social Engineering – Email Phishing:**
   * Phishing emails were sent to employees to determine if they would click malicious links or reveal sensitive information.
4. **Exploitation of SMB Vulnerabilities:**
   * After confirming the vulnerabilities, access was gained through SMB without authentication on the targeted systems.
5. **Remote Shell Installation:**
   * Once the system was accessed, a remote shell was installed to maintain full control over the compromised systems.
6. **Exploration of Sensitive Files:**
   * Files containing patient data and financial information were discovered and accessed using NT Authority-level permissions.

### **4. Conclusion**

The penetration testing results revealed critical security gaps in the hospital's IT infrastructure, including:

* **Severe Vulnerabilities:** SMB EternalBlue allowed full access to critical hospital systems, including McAfee security servers.
* **Unauthorized Access:** Root access enabled exploration of sensitive and confidential patient files.
* **Effective Social Engineering:** Hospital staff were vulnerable to both phone and email phishing attacks.

**Security Impact:**

* The compromise of security servers and access to sensitive files could lead to leaks of personal and financial patient information, and the loss of integrity in the internal network’s security system.

**Recommendations for Mitigating Vulnerabilities:**

1. **Patch SMB Vulnerabilities:** It is essential to apply patches for EternalBlue SMB vulnerabilities on all affected systems.
2. **Secure Internal Networks:** Implement monitoring solutions and restrict access using firewalls to prevent lateral movement.
3. **Employee Training:** Conduct training sessions to educate employees on phishing risks and social engineering tactics.
4. **Review Authentication Processes:** Implement multi-factor authentication for access to critical systems and sensitive data.

### **5. Annexes**

* **Screenshots:** Screenshots demonstrating SMB exploitation and unauthorized access to compromised systems.
* **Technical Documents:** Technical details about SMB vulnerabilities and the specific steps used to exploit them.
* **Access Logs:** Records of penetration testing activities illustrating steps taken to access systems and sensitive files.