Abby Gopal

Lead Pen tester, Cybersecure Inc.

May 28, 2024

**Penetration Test Report**

**Happy Accident Labs (HAL)**

5-28-2024

**2. Report Properties**

**a. Client Information**

Happy Accident Labs (HAL) is the client for this penetration test at 222 S. 15th St, Omaha, NE. The primary contact person is Mr. Bill Winnicott.

**b. Pen testing Company's Information**

Cybersecure Inc. conducted the penetration test. The company is based in Nebraska and can be contacted via its website Cybersecure.com, email at Cybersecure@pentest.com, or phone 1-800-800-8000.

**c. Pen tester Information**

The lead pen tester for this project was Abby Gopal. She can be reached at AbbyGopal@secure.com or 1-800-SECURE.

**3. Report Index**

**a. Table of Contents**

1. Cover Page
2. Report Properties ………………………………………......1
3. Report Index .......................................................... 2
4. Executive Summary .......................................................... 5
5. List of Findings ......................................................... 6
6. Supporting Documentation ......................................................... 8

**b. Table of Figures**

Figure 1: Wireless Attack Detection

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A computer screen with text on it

Description automatically generatedA computer screen with white text

Description automatically generatedFigure 2: Port Scanning DetectioA computer screen shot of a computer screen

Description automatically generatedA computer screen with a black and white text

Description automatically generatedA computer screen shot of a computer screen

Description automatically generatedA computer screen shot of a computer

Description automatically generatedn

A computer screen shot of a computer

Description automatically generated**A computer screen shot of a computer

Description automatically generated**

A computer screenshot of a computer

Description automatically generatedA computer screen shot of a computer

Description automatically generated Figure 3: Vulnerability Scanning Detection

Figure 4: Exploitation Attempts Detection

A computer screen with text on it

Description automatically generatedA computer screen with text on it

Description automatically generated

Figure 5: Credential Harvesting Detection

A screenshot of a computer

Description automatically generated**A computer screen with text on it

Description automatically generated**

A computer screen shot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generatedFigure 6: SQL Injection and XSS Detection

A screen shot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generatedA computer screen with text on it

Description automatically generatedA computer screen with text on it

Description automatically generated**A computer screen with text

Description automatically generated**Figure 7: NetBIOS Enumeration Detection

A computer screen shot of a computer

Description automatically generated

**A screen shot of a computer

Description automatically generated**Figure 8: Backdoor Installation Detection

A close up of a screen

Description automatically generated

**4. Executive Summary**

**a. Objectives**

The primary objective of this penetration test was to identify vulnerabilities within the HAL network and provide actionable recommendations to enhance its security posture.

**b. Scope**

The Scope of this penetration test included all network devices, servers, and endpoints within the HAL network. Systems explicitly defined as out of Scope by HAL were excluded from this test.

**c. Authorizations**

This penetration test was authorized by HAL management, and all activities were conducted within the defined Scope and Timeline.

**d. Assumptions**

The penetration test was conducted based on several assumptions: HAL provided accurate network maps and access credentials, the test environment closely mirrored the production environment, and all activities were monitored by HAL security personnel.

**e. Timeline**

The penetration test began on April 1, 2024, and concluded on April 30, 2024.

**f. Summary of Test**

In simple terms, HAL's initial loss in the penetration test was due to significant vulnerabilities discovered in their systems. These vulnerabilities, like outdated operating systems and insecure configurations, provided easy entry points for attackers. Essentially, HAL's network was like a house with unlocked doors and windows, making it easy for intruders to get in. To break it down further, during the test, which involved various activities, including reconnaissance, vulnerability scanning, exploitation, and post-exploitation, we found that HAL's systems were not adequately updated, leaving them vulnerable to exploitation. Additionally, their network lacked robust monitoring, making detecting and responding to intrusions difficult. Furthermore, weak authentication mechanisms made it easier for attackers to gain unauthorized access to sensitive information.

In essence, HAL's vulnerabilities made it easy for us to breach their network and access critical systems and data, leading to their loss in the penetration test.

**5. List of Findings:**

**High-Level Summary**

| Vulnerability | Impact | Risk |
| --- | --- | --- |
| Outdated Operating Systems | High risk of exploitation due to unpatched vulnerabilities | High |
| Lack of Intrusion Detection and Prevention | Increased risk of undetected attacks | High |
| Insecure Wi-Fi Access Point | Unauthorized access due to weak password practices | High |
| Open Ports (22, 139, 445, 9090) | Unauthorized access, potential exploitation of services | High |
| Vulnerable File Server Services | Unauthorized access to sensitive data | High |

**For detailed technical breakdowns, please refer to the appendix**

Potential Impacts

1. **Data Breach:**
   * Unauthorized access to sensitive data like financial records, intellectual property, or customer information.
   * Potential financial losses, reputational damage, and legal repercussions for HAL.
2. **System Compromise:**
   * Attackers gain full control of critical systems like servers or workstations.
   * Disruption of core business operations, data loss or corruption, and hindered service delivery.
3. **Undetected Intrusions:**
   * Lack of proper monitoring allows attackers to remain undetected for extended periods.
   * Increased potential for data theft, extended system compromise, and wider network infiltration.
4. **Financial Loss:**
   * Costs associated with responding to a security incident, repairing damage, and implementing improved security measures.
   * Potential fines or settlements due to data breaches or non-compliance with regulations.
5. **Reputational Damage:**
   * Loss of customer trust and confidence due to a security breach.
   * Difficulty attracting new business partners and investors.
6. **Productivity Loss:**
   * Disruptions to normal operations caused by security incidents and recovery efforts.
   * Reduced employee productivity and potential delays in project completion.
7. **Legal Issues:**
   * Potential lawsuits from customers or regulators if a security breach exposes sensitive data.
   * The severity of the impact depends on the vulnerabilities exploited and the attackers' goals, with even minor incidents having significant consequences for HAL.

**Technical Impact:**

**Operational Disruption:**

* + Exploitation of vulnerabilities could disrupt critical business operations, leading to service outages, downtime, and unavailability of essential systems and applications.

1. **Data Loss or Corruption:**
   * Successful attacks targeting vulnerable systems may result in the loss or corruption of sensitive data, impacting data integrity and business continuity.
2. **Compromised System Integrity:**
   * Breaches that compromise system integrity could lead to unauthorized modification or deletion of critical files, software, or configurations, posing ongoing security risks.
3. **Exposure to Advanced Threats:**
   * Vulnerabilities left unpatched may expose HAL to advanced threats such as APTs and zero-day exploits, making them difficult to detect and mitigate.
4. **Network Degradation:**
   * Exploitation attempts and unauthorized access may cause increased network traffic, congestion, slowdowns, or instability, impacting performance and availability.
5. **Loss of Confidentiality, Integrity, and Availability (CIA):**
   * Vulnerabilities exploited by attackers can compromise the CIA triad, leading to loss of confidentiality, integrity, and availability of HAL's assets.
6. **Increased Attack Surface:**
   * Vulnerabilities expand the attack surface, making HAL more susceptible to targeted attacks and automated scans from malicious actors.

Recommendations

**High-Level Recommendations**

1. **Update and Patch Systems**: Upgrade all outdated operating systems to supported versions and apply all relevant security patches.
2. **Implement Intrusion Detection and Prevention Systems (IDS/IPS)**: Deploy IDS/IPS to monitor network traffic and detect potential threats in real time.
3. **Enhance Wi-Fi Security**: Use strong, complex passwords for Wi-Fi access points and consider implementing WPA2-Enterprise.
4. **Restrict Open Ports**: Close unnecessary open ports and implement stringent firewall rules to limit exposure.
5. **Secure File Server Configurations**: Ensure proper configurations and regular updates for all file server services to mitigate known vulnerabilities.

Please refer to the appendix for detailed technical breakdowns and specific configuration recommendations.

**Conclusion**

Happy Accident Labs (HAL) faces significant security challenges due to outdated systems, weak configurations, and a lack of proper monitoring. The critical vulnerabilities identified pose a high risk of data breaches, system compromises, and unauthorized access. To address these issues, HAL must implement the recommended actions, including system updates, deployment of IDS/IPS, and enhanced Wi-Fi security. These measures will significantly reduce the risk of security incidents and improve the organization's overall security posture.

**6. Supporting Documentation**

**a. Methodology**

The Methodology for this penetration test included reconnaissance to gather information about the network, scanning to identify vulnerabilities using tools such as Nmap, enum4linux, and Greenbone Vulnerability Management (GVM), exploitation of identified vulnerabilities using Metasploit, and post-exploitation activities to assess the impact of successful exploits.

**b. Tools Used**

The following tools were used during the penetration test:

* Nmap for network scanning and reconnaissance
* Metasploit for vulnerability exploitation
* Greenbone Vulnerability Management (GVM) for vulnerability scanning
* Wi-Fi Pineapple for wireless network assessment
* airodump-ng and aircrack-ng for Wi-Fi password cracking
* enum4linux for SMB enumeration
* Legion

**c. Appendix**

**List of Findings**

| **Vulnerability** | **Affected Hosts/Devices** | **Impact** | **Risk** |
| --- | --- | --- | --- |
| CVE-1999-0519 | 10.19.99.16, 10.19.99.14 | Unauthorized access, potential system crash | High |
| CVE-2017-0143 to CVE-2017-0148 | 10.19.99.10 | Remote code execution, information disclosure | High |
| OS End-of-Life (EOL) | 10.19.99.18, 10.19.99.10, 10.19.99.16, 10.19.99.14 | Unpatched systems are vulnerable | High |
| Lack of Intrusion Detection and Prevention | Entire Network | Increased risk of undetected attacks | High |
| Insecure Wi-Fi Access Point | HAL Wi-Fi Access Point | Unauthorized access due to poor password practices | High |
| Open Ports on Hosts (Port 22) | Multiple hosts | Unauthorized access if not properly secured | Medium |
| Open Ports on Hosts (Ports 139 and 445) | Multiple hosts | Unauthorized access or information disclosure | High |
| Open Port (Port 9090) | One host | Potential vulnerability in the administrative interface | Medium |
| File Server Services | Several hosts | Vulnerable to known exploits | High |
| Operating System Detection | All hosts | Potential vulnerabilities specific to each OS | Low |
| NetBIOS Enumeration | Certain hosts | Potential vulnerabilities in file sharing and authentication | Medium |
| Unauthenticated Vulnerability Scans | All hosts | May reveal vulnerabilities | Medium |
| UDP Scan Results | All hosts | Potential exposure of additional attack surfaces | Medium |
| Potential for Additional Vulnerabilities | All hosts | Further analysis may reveal more vulnerabilities | Low |

**Findings in Detail**

**CVE-1999-0519 (Microsoft Windows SMB/NetBIOS NULL Session Authentication Bypass)**

1. **Definition:** This vulnerability exists due to the misconfiguration of SMB shares on Windows machines. It allows unauthorized access to Windows systems via SMB/NetBIOS NULL Session authentication bypass without valid credentials.
2. **Root Cause:** The presence of enabled guest accounts and improperly configured SMB share permissions.
3. **Proof of Concept:** I used enum4linux to identify and enumerate SMB services running on TCP port 139. We then accessed shared folders without authentication. Refer Figure # 3
4. **Impact:** Unauthorized individuals could access sensitive data and potentially disrupt system operations.
5. **Likelihood:** This vulnerability is highly likely to be exploited due to the availability of public exploits.
6. **Access:** Exploitation typically requires access to the local area network (LAN).
7. **Recommendation:** Disable guest accounts and properly configure SMB permissions to mitigate this vulnerability.

**CVE-2017-0143 to CVE-2017-0148 (Microsoft Windows SMB Server Multiple Vulnerabilities)**

1. **Definition:** These Microsoft Windows SMB server vulnerabilities could allow remote attackers to execute arbitrary code or disclose sensitive information.
2. **Root Cause:** The flawed implementation of the SMB protocol in Microsoft Windows.
3. **Proof of Concept:** Using Metasploit, I targeted vulnerable SMB services. The exploitation led to remote code execution on the target systems. Refer Figure # 3
4. **Impact:** Attackers could gain remote access, steal data, or install malware on the compromised systems.
5. **Likelihood:** These vulnerabilities are highly likely to be exploited due to the existence of readily available exploits.
6. **Access:** Exploitation can be conducted remotely.
7. **Recommendation:** Update all affected systems and disable SMBv1 to mitigate these vulnerabilities.

**OS End-of-Life (EOL)**

1. **Definition:** Operating systems that have reached their end-of-life no longer receive security updates, leaving them vulnerable.
2. **Root Cause:** Continued use of outdated operating systems.
3. **Proof of Concept:** I used Greenbone Vulnerability Management (GVM) to conduct a vulnerability scan and identified several systems running EOL operating systems. Refer Figure # 3
4. **Impact:** These systems are at an increased risk of exploitation and data breaches.
5. **Likelihood:** The likelihood of exploitation is high due to the absence of security patches.
6. **Access:** Access vectors vary depending on the specific vulnerabilities present in the EOL systems.
7. **Recommendation:** Upgrade to supported operating system versions and isolate any remaining EOL systems to minimize risks.

**Lack of Intrusion Detection and Prevention Mechanisms**

1. **Definition:** The absence of intrusion detection and prevention systems (IDS/IPS) hinders the ability to detect and prevent attacks in real time.
2. **Root Cause:** The network lacks sufficient security controls.
3. **Proof of Concept:** During our penetration test, I observed that our activities went undetected by the existing security measures, indicating a lack of effective IDS/IPS. Refer Figure # 8
4. **Impact:** The network is at an increased risk of undetected compromises.
5. **Likelihood:** The likelihood of undetected attacks is high without IDS/IPS.
6. **Recommendation:** Implement IDS/IPS systems and enhance network monitoring to improve threat detection and response capabilities.

**Insecure Wi-Fi Access Point**

1. **Definition:** Weak Wi-Fi password practices allow unauthorized access to the network.
2. **Root Cause:** Poor management of Wi-Fi passwords.
3. **Proof of Concept:** Using tools such as Wi-Fi Pineapple, airodump-ng, and aircrack-ng, I captured the WPA handshake and cracked the password using a wordlist, gaining unauthorized access. Refer Figure # 1
4. **Impact:** Attackers could gain unauthorized access to the network.
5. **Likelihood:** The likelihood of exploitation is high if weak passwords are used.
6. **Recommendation:** Use strong, complex passwords for Wi-Fi access points, update security protocols, and consider implementing WPA2-Enterprise.

**Open Ports on Hosts (Port 22)**

1. **Definition:** The SSH port is open on multiple hosts, potentially allowing unauthorized access to system resources if improperly secured.
2. **Root Cause:** Improper configuration of SSH services, including weak authentication methods.
3. **Proof of Concept:** Accessing SSH services using default or weak credentials. Refer Figure # 2
4. **Impact:** Unauthorized access to sensitive system resources can lead to data breaches or compromise.
5. **Likelihood:** Medium, depending on the strength of SSH configurations and authentication methods.
6. **Recommendation:** Implement strong authentication methods (e.g., public key authentication), regularly update SSH configurations, and enforce access controls.

**Open Ports on Hosts (Ports 139 and 445)**

1. **Definition:** Ports 139 and 445 open on multiple hosts, exposing shared folders and user information, leading to unauthorized access or information disclosure.
2. **Root Cause:** Inadequate configuration of NetBIOS and SMB services, lack of access controls.
3. **Proof of Concept:** Attempting to access shared folders or user information without proper authentication. Refer Figure # 2
4. **Impact:** Unauthorized access to sensitive data, potential information disclosure, and system compromise.
5. **Likelihood:** High, especially if default configurations are used.
6. **Recommendation:** Close unnecessary ports, implement proper access controls and authentication mechanisms, and regularly update and patch SMB services.

**Open Port (Port 9090)**

1. **Definition:** Port 9090 is open on one host, indicating a potential vulnerability in a web-based administrative interface.
2. **Root Cause:** Insecure configuration of the administrative interface.
3. **Proof of Concept:** Scanning and attempting to access the administrative interface on port 9090. Refer Figure # 3
4. **Impact:** Unauthorized access to administrative functions, leading to potential system control or data compromise.
5. **Likelihood:** Medium, depending on the security measures in place for the administrative interface.
6. **Recommendation:** Secure the administrative interface with strong authentication, restrict access to trusted IP addresses, and regularly update the administrative application.

**File Server Services**

1. **Definition:** Several hosts are running file server services vulnerable to known exploits.
2. **Root Cause:** Use of outdated file server software or insecure configurations.
3. **Proof of Concept:** Using tools to identify and exploit vulnerabilities in file server services. Refer Figure #
4. **Impact:** Unauthorized access to sensitive files, data breaches, or malware distribution.
5. **Likelihood:** High, particularly if known vulnerabilities are not patched.
6. **Recommendation:** Update file server software to the latest versions, configure services securely, and implement strict access controls.

**Operating System Detection**

1. **Definition:** Potential vulnerabilities specific to each detected operating system.
2. **Root Cause:** Presence of outdated or misconfigured operating systems.
3. **Proof of Concept:** Conducting network scans to identify operating systems and their configurations. Refer Figure # 2
4. **Impact:** Increased risk of exploitation due to OS-specific vulnerabilities.
5. **Likelihood:** Low but varies based on OS versions and configurations.
6. **Recommendation:** Regularly update and patch all operating systems, implement secure configurations, and monitor for vulnerabilities.

**NetBIOS Enumeration**

1. **Definition:** Potential vulnerabilities in file sharing and authentication services due to exposed NetBIOS information.
2. **Root Cause:** Misconfigured NetBIOS services.
3. **Proof of Concept:** Using enumeration tools to gather information about shared resources and user accounts. Refer Figure # 7
4. **Impact:** Unauthorized access to shared resources, potential data leakage, or credential harvesting.
5. **Likelihood:** Medium, especially if default configurations are used.
6. **Recommendation:** Restrict NetBIOS services, implement proper access controls, and disable unnecessary services.

**Unauthenticated Vulnerability Scans**

1. **Definition:** Unauthenticated scans reveal potential vulnerabilities on the network.
2. **Root Cause:** Inadequate security measures and configurations.
3. **Proof of Concept:** Conducting unauthenticated vulnerability scans to identify potential weaknesses. Refer Figure # 3,4,5
4. **Impact:** Attackers may identify and exploit vulnerabilities without needing credentials.
5. **Likelihood:** Medium, depending on the effectiveness of existing security controls.
6. **Recommendation:** Strengthen security measures, regularly conduct authenticated vulnerability scans, and address identified vulnerabilities promptly.

**UDP Scan Results**

1. **Definition:** Exposure of additional attack surfaces through open UDP ports.
2. **Root Cause:** Improperly secured UDP services.
3. **Proof of Concept:** Conducting UDP scans to identify open ports and potentially vulnerable services. Refer Figure # 2
4. **Impact:** Increased risk of exploitation through less commonly secured UDP services.
5. **Likelihood:** Medium, particularly if UDP services are not regularly monitored or secured.
6. **Recommendation:** Regularly monitor and secure UDP services, close unnecessary ports, and implement appropriate firewall rules.

**Potential for Additional Vulnerabilities**

1. **Definition:** Further analysis may reveal more vulnerabilities beyond those identified in the initial penetration test.
2. **Root Cause:** Limited Scope or depth of initial testing.
3. **Proof of Concept:** Acknowledge potential gaps in the initial testing process.
4. **Impact:** Undetected vulnerabilities may remain, posing ongoing risks.
5. **Likelihood:** Low, but ongoing vigilance is necessary.
6. **Recommendation:** Conduct regular, comprehensive security assessments and continuously improve security measures.

Thank you for contacting us regarding the HAL network penetration test. We understand your concerns about the potential lack of detection of our activities and appreciate the opportunity to address them. As requested, our final report will include a comprehensive section on detecting network intrusions tailored specifically to Happy Accident Labs (HAL). Drawing from our penetration test activities and NIST SP 800-61, we provide insights into detecting network intrusions and enhancing the overall HAL organization security posture. In our penetration test activities, several actions could have been detected from the HAL user end with appropriate monitoring and detection mechanisms in place.

Some Indicators of Network Intrusions are unusual network traffic patterns, Abnormal spikes in network traffic, or unexpected data flows that can indicate unauthorized activities. During penetration tests, activities like port scanning, enumeration, and exploitation may generate anomalous traffic patterns that are detectable through continuous network monitoring. Unexpected system crashes, slowdowns, or configuration changes may signify unauthorized access or malicious activity. HAL organization should monitor security logs for unusual activities, including repeated login failures, privilege escalation attempts, or suspicious file access patterns, which is crucial for detecting intrusions. HAL organization should regularly review firewalls, IDS/IPS, and network device logs to identify potential threats and security incidents. The penetration test employed various techniques to exploit vulnerabilities in HAL's systems. These techniques included:

Wireless Attacks: Utilized a Wi-Fi pineapple to scan access points and capture the WPA handshake. Identified the HAL WIFI access point using airodump-ng. Cracked the WPA handshake using aircrack-ng and the rockyou.txt wordlist. The command used: aircrack-ng --b F8:32: e4:52:ca: F8 -w /usr/share/wordlists/rockyou.txt HAL. Cap. Result: PSK found the key -""huskersare#""

Detection Method: HAL's wireless intrusion detection system (WIDS) could have flagged this suspicious behavior, such as unauthorized devices attempting to intercept Wi-Fi traffic or performing de-authentication attacks.

Port Scanning: The test used Nmap to identify and determine the local machine's IP address using ipconfig. We conducted a ping sweep using Nmap -sP 10.19.99.1-100 to identify live hosts on the subnet. Full open and stealth scans were performed to identify open ports on each live host. Commands used: Nmap -v -sP 10.19.99.1-100, Nmap -v -sS -O 10.19.99.1-100, and the results Identified live hosts and open ports on each host, along with potential operating systems.

Detection Method: Network Intrusion Detection Systems (NIDS) can analyze network traffic for suspicious patterns indicative of port scanning, such as a high volume of connection attempts within a short timeframe. Additionally, firewall logs can reveal repeated connection attempts from a single IP address, suggesting reconnaissance activities.

Vulnerability Scanning: Conducted vulnerability scans with tools like Greenbone Vulnerability Management (GVM)and the EternalBlue exploits toidentify weaknesses in HAL's systems. It details the findings from the GVM scan across seven active hosts on the HAL network. The scan identified high-severity vulnerabilities on multiple hosts. Critical vulnerabilities include CVE-1999-0519, a Microsoft Windows SMB/NetBIOS NULL Session that allows unauthorized access. CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148: Microsoft Windows SMB Server multiple vulnerabilities allowing remote code execution. Additionally, all scanned hosts ran operating systems past their end-of-life (EOL), making them more vulnerable to vulnerabilities.

Detection Method: Intrusion detection systems can flag the use of vulnerability scanning tools by analyzing network traffic for signatures associated with these tools. Furthermore, sudden spikes in network traffic or unusual scanning patterns can trigger alerts for ongoing vulnerability assessments.

Exploitation Attempts: The penetration test involved attempts to exploit known vulnerabilities, such as MS17-010, using Metasploit to gain unauthorized access to HAL systems.

Detection Method: Intrusion detection systems should monitor for repeated failed login attempts, brute-force attacks, or unexpected access to critical systems or resources.

Credential Harvesting: Employing techniques like SMB enumeration or password spraying attacks using John the Ripper to harvest user credentials.

Detection Method: Monitoring authentication logs for multiple failed login attempts can help detect credential harvesting attempts. Security measures like account lockout policies can mitigate the risk of successful credential theft.

SQL Injection and XSS Attacks: Exploiting vulnerabilities in web applications to execute SQL injection or XSS attacks.

Detection Method: Web application firewalls (WAFs) can inspect incoming web traffic for suspicious patterns indicative of SQL injection or XSS attacks. Furthermore, conducting thorough code reviews and implementing input validation can prevent such attacks.

NetBIOS Enumeration: Using enum4linux to probe hosts with active NetBIOS services for information about shares, users, and groups.

Detection Method: HAL's SIEM (Security Information and Event Management) system could have detected anomalies in network traffic, system logs, or user activities by applying machine learning algorithms or statistical analysis to detect deviations from baseline behaviors.

Backdoor Installation: A backdoor, such as Netcat (nc), was installed on HAL's systems to maintain persistent access. We then used nc -v <target\_ip> 1999 command to connect to the specified IP address on port 1999, where the backdoor is listening.

Detection Method: Monitoring the Security Information and Event Management (SIEM) system can help detect backdoor installations. Endpoint security solutions with behavior-based detection capabilities can identify suspicious processes or system changes indicative of backdoor activity.

Some of the overall processes for detecting network intrusions can be achieved by implementing intrusion detection and prevention systems (IDS/IPS), network traffic analyzers, and log monitoring solutions to monitor the network continuously for signs of intrusion. By understanding typical network traffic patterns, system performance metrics, and user behaviors, HAL organizations can quickly detect anomalies indicative of intrusions. Anomaly detection solutions can analyze large volumes of data in real-time, flagging suspicious behaviors for further investigation. Continuous Monitoring and Developing a plan to test incident response regularly will ensure that the HAL organization is prepared to respond effectively to network intrusions.

In summary, HAL organizations should implement a multi-layered detection strategy incorporating network monitoring, intrusion detection systems, log analysis, and user behavior monitoring to detect and respond to network intrusions effectively. In addition to the detection strategies we previously discussed, HAL can implement several advanced measures to boost its network security. Network segmentation can help contain potential intrusions by dividing the network into smaller, isolated segments. Deploying Endpoint Detection and Response (EDR) solutions will enable continuous monitoring and threat response at the endpoint level. Integrating threat intelligence feeds keeps the organization informed about the latest threats. At the same time, User and Entity Behavior Analytics (UEBA) tools can detect anomalies and insider threats by analyzing typical behavior patterns.

Establishing a Security Operations Center (SOC) for round-the-clock monitoring. Regular security audits and vulnerability assessments help identify and fix potential weaknesses. Strengthening policies and procedures is also crucial. Developing and updating an incident response plan, providing ongoing cybersecurity training for employees, enforcing the principle of least privilege, and implementing multi-factor authentication (MFA) add layers of defense.

By combining these advanced measures, HAL Organization can significantly enhance its ability to detect, prevent, and respond to network intrusions. Our penetration test activities serve as a roadmap to identify vulnerabilities and strengthen HAL's security posture. Please feel free to reach out if you need further clarification or assistance with the detection mechanisms outlined in our report.

**d. References**

1. Cichonski, P., et al. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication.
2. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115.
3. Offensive Security (2023). Kali Linux Tools. Offensive Security's website.

**e. Glossary**Top of Form

**Authentication**  
The process of verifying the identity of a user, device, or other entity in a computer system.

**Authorization**  
The process determines what actions an authenticated user, device, or other entity can perform.

**Backdoor**  
A method by which an authorized or unauthorized user can bypass normal security controls to access a computer system or data.

**Brute Force Attack**  
A trial-and-error method is used to decode encrypted data such as passwords by trying a large number of possible combinations.

**Credential Harvesting**  
The act of collecting login credentials (usernames and passwords) through various methods, including phishing and malware.

**Cross-Site Scripting (XSS)**  
A type of security vulnerability typically found in web applications where an attacker injects malicious scripts into content from otherwise trusted websites.

**CVE (Common Vulnerabilities and Exposures)**  
A list of publicly disclosed information security vulnerabilities and exposures.

**Denial of Service (DoS) Attack**  
An attack is meant to shut down a machine or network, making it inaccessible to its intended users.

**Detection**  
The process of identifying potential security breaches or incidents.

**Enumeration**  
The process of extracting information about a system, such as usernames, machine names, network resources, shares, and services.

**Firewall**  
A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

**Host**  
Any computer connected to a network includes servers, workstations, network devices, and others.

**Intrusion Detection System (IDS)**  
A device or software application that monitors a network or systems for malicious activity or policy violations.

**Intrusion Prevention System (IPS)**  
A form of network security that works to detect and prevent identified threats.

**Malware**  
Software designed to disrupt, damage, or gain unauthorized access to a computer system.

**NetBIOS (Network Basic Input/Output System)**  
A program that allows applications on different computers to communicate within a local area network (LAN).

**Penetration Test (Pen Test)**  
A simulated cyber-attack against a computer system is performed to evaluate the system's security.

**Port Scanning**  
A technique used to identify open ports and services available on a networked device.

**Reconnaissance**  
The preliminary information-gathering phase in a penetration test involves collecting information about the target system to identify potential entry points.

**SQL Injection**  
A code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques.

**Threat**  
A potential cause of an unwanted impact on a system or organization.

**Unauthorized Access**  
Gaining access to systems, networks, or data without permission.

**Vulnerability**  
A weakness in a system or its design that could be exploited by a threat actor, such as an attacker, to compromise the system.

**Vulnerability Scanning**  
An automated process of proactively identifying security vulnerabilities in a system.

**Wi-Fi Pineapple**  
A wireless auditing tool designed to help network administrators with network security assessments.

References

*Penetration Test Report MegaCorp One Offensive Security Services, LLC*. (2013). <https://www.offsec.com/reports/sample-penetration-testing-report.pdf>

*Pentest Report Outline*. (n.d.). <https://content.bellevue.edu/cst/cybr/430_block/Documents/Pentest_Report_Outline(1).pdf>

*Tips for Creating a Strong Cybersecurity Assessment Report*. (n.d.). Zeltser.com. <https://zeltser.com/security-assessment-report-cheat-sheet/>

Bottom of Form