LIGHTHOUSE LAB

CYBERSECURITY

CAT’S COMPANY VULNERABILITIES

DANIEL O. OLUWAYALE

CONTENT Page

Executive Summary

The purpose of this vulnerability assessment was to identify and analyze potential security risks in the IT infrastructure of Cat's Company. Using a variety of tools, including OpenVAS, several vulnerabilities were detected across various systems. These vulnerabilities pose risks ranging from moderate to severe, with some requiring immediate attention due to their high impact on confidentiality, integrity, and availability of the systems.

The findings indicate issues such as weak FTP security, unencrypted data transmission, and information leakage through timestamp-based attacks. Based on the severity of the vulnerabilities, the report provides recommendations for mitigating these risks, including securing FTP access, enforcing encryption protocols, and addressing information disclosure vulnerabilities. The recommendations are prioritized based on risk level, ensuring that the executive team can allocate resources effectively for remediation.

The scan results from OpenVAS revealed a range of vulnerabilities categorized by their severity. Below is a summary of the findings:

Scan Result

1. FTP Brute Force Logins (Severity: 7.5 - High)
   This vulnerability allows attackers to potentially gain unauthorized access easily to FTP services using brute force techniques. When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct. MITRE. (Dec 15, 2024). It is critical because it could lead to complete access to sensitive company data stored on the server.

2. Anonymous FTP Login Reporting (Severity: 6.4 - Medium)
   The server allows anonymous FTP logins, which pose a security risk by enabling unauthorized users to access files. The product constructs the name of a file or other resource using input from an upstream component, but it does not restrict or incorrectly restricts the resulting name. MITRE. (Dec 15, 2024). While this is not as severe as a brute force attack, it still exposes the company to unnecessary risk.

3. FTP Unencrypted Cleartext Login (Severity: 4.8 - Medium)
   FTP login credentials are transmitted in cleartext, making them vulnerable to interception by attackers. The product transmits sensitive or security-critical data in clear text in a communication channel that can be sniffed by unauthorized actors. MITRE. (Dec 15, 2024). This issue should be addressed to prevent potential data breaches.

4. Cleartext Transmission of Sensitive Information via HTTP (Severity: 4.8 - Medium)
Similar to the FTP issue above, this vulnerability occurs when HTTP (instead of HTTPS which is the secured version) is used to transmit sensitive data such as usernames, passwords, or financial data, which can be intercepted by attackers. The product transmits sensitive or security-critical data in clear text in a communication channel that can be sniffed by unauthorized actors. MITRE. (Dec 15, 2024).

5. TCP Timestamps Information Disclosure (Severity: 2.6 - Low)
TCP timestamps leak information that could potentially aid in network reconnaissance. This is considered a low-risk vulnerability but should still be mitigated to minimize data exposure. Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel. MITRE. (Dec 15, 2024).

6. ICMP Timestamp Reply Information Disclosure (Severity: 2.1 - Low)
The system responds to ICMP timestamp requests, disclosing system time details. The product generates an error message that includes sensitive information about its environment, users, or associated data. While this does not directly compromise security, it could aid attackers in gathering information for more sophisticated attacks. MITRE. (Dec 15, 2024).

Methodology

The vulnerability assessment was conducted using OpenVAS, a comprehensive and industry-standard tool for vulnerability scanning. OpenVAS is an open-source Linux-based vulnerability scanner supported by a community spearheaded by the German organization Greenbone Networks. Lighthouse (Dec 15, 2024). The scan was performed in a controlled environment, targeting both internal and external systems connected to the company network.

Each scan was tailored to assess specific risk factors such as open ports, services, misconfigurations, and weaknesses in protocols like FTP and HTTP. The following tools were utilized:

- OpenVAS: Used to perform a full vulnerability scan across the network, including detecting weak authentication methods, cleartext data transmission, and protocol weaknesses.
- NIST and MITRE frameworks: Applied to assess and prioritize the vulnerabilities found, ensuring they were categorized appropriately based on potential risk to business operations.

Findings

The scan successfully identified the following systems and vulnerabilities:

- FTP Service: Multiple issues related to FTP login security were found, including unencrypted logins and the ability to perform brute force attacks.
- HTTP and ICMP Services: Disclosures related to sensitive information via unencrypted HTTP and timestamp-based ICMP replies were detected.
- System Configuration: Certain network configurations allowed unnecessary information leakage, which could be exploited by attackers to gain insights into the system.

Risk Assessment

The vulnerabilities identified were categorized into the following severity levels:

- Critical (7.5):
  - FTP Brute Force Login: This represents a major risk to system integrity, as unauthorized access could allow attackers to manipulate or steal critical company data.
- High (6.4):
  - Anonymous FTP Login: While this doesn’t immediately allow unauthorized access, it opens doors to further attacks and data exfiltration.
- Medium (4.8):
  - FTP Unencrypted Cleartext Login and Cleartext Transmission of Sensitive Information via HTTP: These vulnerabilities could result in data breaches if intercepted by attackers.
- Low (2.6 and 2.1):

- TCP Timestamps and ICMP Timestamp Reply Information Disclosure: These are low impact vulnerabilities but addressing them can reduce the overall attack surface.

Recommendations

1. Implement FTP Authentication Security (High Priority):
    - Enforce strong password and consistent password update policies and consider using more secure protocols like SFTP or FTPS. Disable anonymous FTP logins to ensure only authorized users can access critical systems. Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services. MITRE Corporation (Dec 15, 2024).
2. Encrypt All Data in Transit (High Priority):
    - Transition from HTTP to HTTPS for all sensitive data transmission. Ensure that FTP logins use secure methods (SFTP, FTPS) to protect credentials from interception. Enable FTPS or enforce the connection via the 'AUTH TLS' command. Doe, J. (2024).
3. Disable ICMP Timestamps (Medium Priority):
    - Disable ICMP timestamp replies to prevent attackers from gaining information about system time, which could be useful in launching time-based attacks. Disable the support for ICMP timestamp on the remote host completely. Doe, J. (2024).
4. Apply System Patches and Updates (Medium Priority):
    - Ensure that all systems are up to date with the latest security patches to address known vulnerabilities and minimize the risk of exploitation.
5. Review and Update Security Policies (Medium Priority):
    - Review current security policies regarding access controls, data encryption, and system monitoring. Update policies to reflect the latest best practices for securing sensitive data and services. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. Consider blocking risky authentication requests, such

as those originating from anonymizing services/proxies. MITRE Corporation. (Dec 16, 2024).

References

MITRE. (Dec 15, 2024). *CWE-287: Improper Authentication*. The MITRE Corporation. https://cwe.mitre.org/data/definitions/287.html

MITRE. (Dec 15, 2024). *CWE-641: Improper Restriction of Input During Web Page Generation ('Injection')*. The MITRE Corporation. https://cwe.mitre.org/data/definitions/641.html

MITRE. (Dec 15, 2024). *CWE-319: Cleartext Transmission of Sensitive Information*. The MITRE Corporation. https://cwe.mitre.org/data/definitions/319.html

MITRE. (Dec 15, 2024). *Observable Discrepancy Between Code and Documentation*. The MITRE Corporation. https://cwe.mitre.org/data/definitions/203.html

MITRE. (Dec 15, 2024). *CWE-209: Information Exposure Through an Error Message.* The MITRE Corporation. https://cwe.mitre.org/data/definitions/209.html

Lighthouse (Dec 15, 2024). *W05D3 - Activity 3020*. Lighthouse Labs. https://web.compass.lighthouselabs.ca/p/cyber/days/w05d3/activities/3020

MITRE Corporation. *T1110: Brute Force*. MITRE ATT&CK. Retrieved December 15, 2024, from https://attack.mitre.org/techniques/T1110/

Doe, J. (2024). *Security report on vulnerability assessments*. Retrieved from https://127.0.0.1:9392/report/930ef5f9-ada3-46d3-8ae1-9a0efd19b2f9

MITRE Corporation. *T1110: Brute force*. MITRE ATT&CK. Retrieved December 15, 2024, from https://attack.mitre.org/techniques/T1110/