Cat's Company Vulnerabilities Report

Daniel Deng

Table of Contents

Executive Summary:

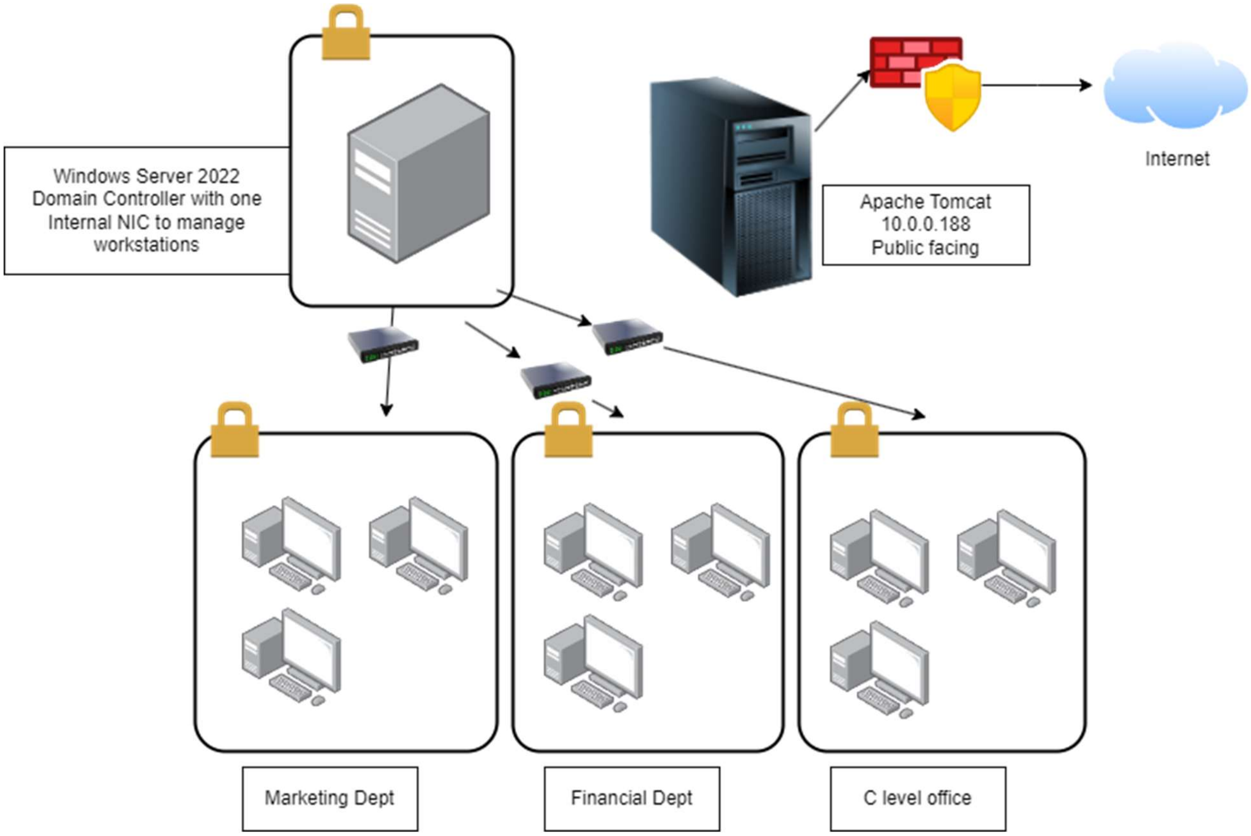
Cat's company, which provides essential pet services for the city, is experiencing rapid growth and business expansion, leading to an increase in both internal and external cyber threats. As the company scales, the complexity of its IT infrastructure and the potential attack surface also expand, making it more vulnerable to security breaches. Recognizing the heightened risk, Cat sought our expertise for a comprehensive vulnerability scan to identify and mitigate potential security weaknesses. By addressing these vulnerabilities proactively, the company aims to safeguard its assets and maintain robust security as it continues to grow.

In our recent vulnerability assessment targeting Cat company's Linux-based server and internal networks, we employed professional tools to conduct comprehensive scans of our systems during non-production hours to minimize disruption. This evaluation identified several critical vulnerabilities that pose potential risks to Cat organization's security and operations. The vulnerabilities were prioritized based on the level of risk they represent according to priority level, with a focus on issues that could lead to data breaches, service disruptions, or unauthorized access.

To ensure the security of the systems, we recommend immediate action on the highest-risk vulnerabilities. This includes updating and patching affected systems, enhancing network security protocols, and implementing regular monitoring and auditing processes. Addressing these issues promptly will mitigate potential threats, protect sensitive data, and maintain the integrity and availability of our services. By taking these steps, we can significantly reduce our risk exposure and strengthen our overall security posture.

Company Topology:

(Note: This is a hypothetical scenario created for demonstration purposes related to reporting.)



Methodology:

The scan methodology employed Tenable Nessus, a leading vulnerability scanning tool, to evaluate vulnerabilities on the company's Apache server at IP address 10.0.2.188 and within the internal network (4 subnets). An authenticated scan was conducted to ensure thorough coverage, with each scan, tool, and test designed to uncover potential security weaknesses.

The scan was conducted at midnight to avoid peak production hours, with clear communication made with the company beforehand. This thorough approach ensured that the scan was both effective and minimally disruptive to the company's operations.

Scan Results:

After conducting a systematic scan, multiple vulnerabilities were identified on the company's public-facing Apache server, some of which carry very high CVSS scores and require immediate remediation. Additionally, critical vulnerabilities were found within the internal network across various departments. The primary vulnerabilities of the Apache server detected include the following:

- An unsupported version of Apache Tomcat is installed.
- The SSH host keys are weak.
- The SSL certificate uses a weak key.

These vulnerabilities significantly expose the company's assets to threats, including unauthorized access, data breaches, and remote code execution. Even though a firewall has been implemented, it is not enough to fully mitigate these risks. Immediate remediation is necessary to protect the integrity and security of the company's critical infrastructure.

The company's internal network has been found to contain several vulnerabilities, all with high CVSS scores. While these vulnerabilities are inside the Marketing dept subnet within the internal network, the immediate priority is to mitigate the public-facing Apache server vulnerability, as it poses the most direct risk due to its exposure to the internet.

Following the mitigation of the Apache server, attention will shift to addressing the internal network vulnerabilities. Although these internal systems are not directly accessible from the internet, the potential for insider threats within the internal network must be considered and addressed to ensure comprehensive protection.

The vulnerabilities found in the internal network include:

- IRC server on the Marketing dept workstation is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host
- A VNC server running in the Marketing dept subnet is secured with a weak password.

Findings:

Public-facing Apache server:

An unsupported version of Apache Tomcat is installed:

1. Known Vulnerabilities:

- **Exploitable Flaws:** Unsupported versions of Apache Tomcat are no longer receiving security updates or patches. This leaves the server vulnerable to known security flaws that attackers can exploit, such as remote code execution, privilege escalation, and information disclosure vulnerabilities.
- **CVE-2013-6357:** Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST method, as demonstrated by a /manager/html/undeploy?path= URI (NVD, CVE-2013-6357 Detail, n.d.).

2. Compliance Issues:

- **Regulatory Non-Compliance:** Running unsupported software can lead to non-compliance with industry regulations and standards, such as PCI-DSS, HIPAA, or GDPR. This can result in fines, legal liabilities, or loss of certification.
- **Audit Failures:** Organizations may fail security audits, leading to reputational damage and potential financial penalties.

3. Increased Attack Surface:

- **Wider Target for Attackers:** Unsupported versions may contain multiple unpatched vulnerabilities, increasing the attack surface. This makes it easier for attackers to find and exploit weaknesses in the system.
- **Botnet Recruitment:** The server could be compromised and added to a botnet, which could be used for malicious activities like distributed denial-of-service (DDoS) attacks.

4. Data Breach Risks:

- **Sensitive Data Exposure:** If the unsupported Apache Tomcat instance is compromised, attackers could gain unauthorized access to sensitive data, leading to potential data breaches.
- **Credential Theft:** Attackers could steal login credentials or other sensitive information stored or transmitted through the server, which could be used for further attacks.

5. Operational Disruptions:

- **Service Downtime:** Exploiting vulnerabilities in an unsupported version could lead to service disruptions, causing downtime for critical applications and impacting business operations.
- **Malware Infections:** The server might be used to host or spread malware, affecting not only the server itself but also other connected systems.

The SSH host keys are weak:

1. Unauthorized Access:

- **CVE-2008-0166:** OpenSSL(library for implementing cryptographic functions for SSH) 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys (NVD, CVE-2008-0166 Detail, n.d.).
- **Server Compromise:** If an attacker successfully exploits weak SSH keys, they could gain unauthorized access to the server, allowing them to execute commands, steal sensitive data, or manipulate the server's operations.

2. Data Breach:

- **Sensitive Information Exposure:** Weak SSH keys could lead to a data breach, where attackers gain access to confidential information, including personal data, financial records, or proprietary company information.
- **Data Integrity:** Attackers could also alter or delete data, leading to data integrity issues that could disrupt operations or cause significant damage.

The SSL certificate uses a weak key.

1. Encryption Weakness:

- **Data Decryption:** A weak key can make the encrypted data vulnerable to decryption by attackers. They can intercept and decrypt sensitive information, such as login credentials, financial data, or personal information, compromising the confidentiality of the data transmitted between the server and clients.
- **Eavesdropping:** Attackers can more easily break the encryption, allowing them to eavesdrop on the communication, gaining access to private conversations or transactions.

2. Brute force:

- **CVE-2008-0166:** OpenSSL(library for implementing cryptographic functions for SSH) 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys (NVD, CVE-2008-0166 Detail, n.d.).

Internal Network:

IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host

An IRC (Internet Relay Chat) server is a system that facilitates real-time communication over the network through text-based chat. IRC servers host chat rooms, known as channels, where users can join, exchange messages, and participate in discussions.

1. Remote Code Execution

- **CVE-2010-2075 Detail:** UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands (NVD, CVE-2010-2075 Detail, n.d.).

2. Potential Data Exfiltration:

- **Unauthorized Access:** Attackers could leverage the backdoor to access confidential information stored on Marketing department workstations or other connected systems. This could lead to data breaches and the exposure of sensitive company or customer data.

A VNC server running in the Marketing dept subnet is secured with a weak password.

A VNC (Virtual Network Computing) server is a system that allows remote access and control of a computer's desktop environment (GUI) over a network.

Weak password:

- The VNC server running on the remote host is secured with a weak password. Nessus was able to log in using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Recommendation:

For Public-facing Apache Server:

1 Upgrade Apache Tomcat:

- Update to the Latest Supported Version: Immediately upgrade to the latest stable and supported version of Apache Tomcat. This ensures that you have the latest security patches and features. You can download the latest version from the official Apache Tomcat website.
- Check Compatibility: Before upgrading, ensure that your applications are compatible with the new version of Tomcat. Review the migration guide provided by Apache to help with the upgrade process.

2 **Update OpenSSL:**

- **Upgrade to a Secure Version:** Immediately update OpenSSL to a version that has fixed the vulnerability.
- **Package Management:** Use your system's package management tools (e.g., apt-get for Debian-based systems) to install the updated OpenSSL version:

  ```
  sudo apt-get update

  sudo apt-get upgrade openssl
  ```

3 **Regenerate Cryptographic Keys:**

- **Generate New Keys:** After updating OpenSSL, all cryptographic keys that were generated using the vulnerable versions should be regenerated. This includes SSL/TLS certificates, SSH keys, and any other keys used for securing communications.
- **Reissue Certificates:** If SSL/TLS certificates were generated with the flawed RNG, contact your Certificate Authority (CA) to revoke and reissue the certificates.

For Internal Network:

1 Upgrade IRC server and software:

- Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

2 Secure the VNC service with a strong password.

- Implement a Strong password policy: requiring a minimum of 12 characters, including a mix of uppercase letters, lowercase letters, numbers, and special characters, the password must expire every 6 months, or a breach has occurred.

The marketing department's subnet is internally protected by switches and firewalls, which minimizes external risks. However, the potential for insider threats within this internal network still needs to be considered. **The priority should be focused on the company's public-facing Apache server.**

References:

NVD. (n.d.). *CVE-2008-0166 Detail*. Retrieved from CVE-2008-0166 Detail: https://nvd.nist.gov/vuln/detail/CVE-2008-0166

NVD. (n.d.). *CVE-2010-2075 Detail*. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2010-2075

NVD. (n.d.). *CVE-2013-6357 Detail*. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2013-6357